Università degli Studi di Padova

DIPARTIMENTO DI DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Magistrale in Matematica

Tesi di laurea magistrale

p-adic methods for rational points on curves of genus $g \geq 2$

Candidato:

Luca Ferrigno

Matricola 1232185

Relatore:

Prof. Matteo Longo

Anno accademico 2020 - 2021

24/09/2021

Introduction

One of the oldest problems in mathematics is the study of *Diophantine equations*, that is the study of solutions of (systems of) polynomial equations with integer coefficients

$$f(X_1, X_2, \ldots, X_n) = 0$$

in integers, rational numbers, or sometimes more general number rings. This is a problem that has been studied since the dawn of mathematics, with examples in texts of the ancient Babylonians, Chinese, Egyptians and Greeks. The interesting thing about those equations is that understanding the rational and integer solutions to seemingly simple Diophantine equations, like

$$x^n + y^n = z^n \qquad \text{for } n \geq 3$$

often involves unexpectedly advanced tools, and sometimes yields to the creation of new tools or even new areas of research.

At first, Diophantine equations were mainly studied using algebraic tools. However, at the start of the 20th century, with the development of modern algebraic geometry, mathematicians started to realize that those equations define algebraic varieties and, therefore, they could use the geometric properties of the associated variety to deduce arithmetic properties of the Diophantine equation. Hence, integer or rational solutions of Diophantine equations correspond to points with integral or rational coordinates on the corresponding varieties. This area of research is now called *Diophantine geometry*.

The simplest case to study (and the main focus of this thesis) is when the associated variety has dimension 1, i.e. it is a curve. We will see that for every curve $\mathcal{C}$, there exists a non-negative integer $g \geq 0$, called the *genus of* $\mathcal{C}$ (see Definition 1.39). In this case, the genus fully characterizes the properties of $\mathcal{C}(\mathbb{Q})$, the set of rational points[1] of $\mathcal{C}$.

Curves of genus 0. For (smooth, projective) curves $\mathcal{C}$ of genus $g = 0$ defined over $\mathbb{Q}$, the study of rational points is particularly easy, since the Riemann-Roch theorem (Theorem 1.38) implies that every such curve is isomorphic over $\mathbb{Q}$ to a (possibly degenerate) conic C in $\mathbb{P}^2$ (see [46, Theorem A.4.3.1] for a proof). Moreover, if $C(\mathbb{Q}) \neq \emptyset$, then we can also prove that it is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$.

[1] We could be more general and work over a number field K instead of $\mathbb{Q}$. All theorems would be (almost) the same but, for ease of exposition, we will continue to work over $\mathbb{Q}$.

The argument is very easy: suppose that this conic has at least one rational point. Up to a change of coordinates, we can assume that this point is $P_0 = [0, 0, 1]$. Therefore the conic has equation

$$C/\mathbb{Q} : aX^2 + bXY + cY^2 + dXZ + eYZ = 0$$

with $a, b, c, d, e \in \mathbb{Z}$, $(a, b, c) \neq (0, 0, 0)$, $(d, e) \neq (0, 0)$ (otherwise it would be either a line or the union of two lines, which is an even easier case to study). Notice that for every rational point $P \in C(\mathbb{Q})$, the line through P and P_0 has rational coefficients and, conversely, the line with equation $tX + uY = 0$ ($[t, u] \in \mathbb{P}^1(\mathbb{Q})$) intersects the conic at the points $[0, 0, 1]$ and $\left[du^2 - etu, -dtu + et^2, -(au^2 - btu + ct^2)\right]$.

This defines an isomorphism:

$$\begin{aligned} \Phi : \mathbb{P}^1(\mathbb{Q}) &\longrightarrow C(\mathbb{Q}) \\ [t, u] &\longmapsto \left[du^2 - etu, -dtu + et^2, -(au^2 - btu + ct^2)\right] \end{aligned}$$

So, the only thing left to do in this case is determining if $C(\mathbb{Q}) = \emptyset$. Luckily, we have the following theorem

Theorem 0.1 (Hasse-Minkowski)**.** *$C(\mathbb{Q}) \neq \emptyset$ if and only if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for every prime p.*

Curves of genus 1. A genus one curve over $\mathbb{Q}$ with a rational point $\mathcal{O}$ is called an *elliptic curve*. Again, using the Riemann-Roch Theorem (see [68, Proposition III.3.1] for a proof), we can show that an elliptic curve E over $\mathbb{Q}$ is isomorphic (over $\mathbb{Q}$) to a smooth plane curve with equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

More importantly, it can be shown that E can be given the structure of an algebraic group [68, Chapter III]. In this case, the Mordell-Weil theorem (Theorem 1.50) tells us that the group of rational points $E(\mathbb{Q})$ is actually a finitely generated abelian group, i.e. we have:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$$

where $E(\mathbb{Q})_{tors}$ is the (finite) subgroup of points of finite order. Computing the torsion subgroup is quite easy, and we know a lot about it. For example:

Theorem 0.2 (Nagell-Lutz)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$ and $4a^3 + 27b^2 \neq 0$, and let $P \in E(\mathbb{Q})$ a non trivial torsion point, then:*

1. *$x(P), y(P) \in \mathbb{Z}$*
2. *Either $2P = \mathcal{O}$ or $y(P)^2$ divides $4a^3 + 27b^2$*

Theorem 0.3 (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve. Then the subgroup $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \qquad & \text{with } 1 \leq n \leq 10 \text{ or } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \qquad & \text{with } 1 \leq n \leq 4 \end{aligned}$$

On the other hand, computing the generators of infinite order is much more difficult. There are some algorithms that work really well in practice [68, Chapter X], but we do not know if they work for every elliptic curve.

Curves of genus ≥ 2. In contrast with the previous cases, in 1922 Mordell [57] conjectured the following result, which was first proven by Faltings [37] in 1983.

Theorem 0.4 (Faltings). *Let $\mathcal{C}/\mathbb{Q}$ be a curve of genus $g \geq 2$. Then $\mathcal{C}(\mathbb{Q})$ is finite.*

Faltings' theorem was later proved independently by Vojta [79] , using Diophantine approximation, and simplifications of Vojta's proof were found by Faltings and by Bombieri, who presented a relatively elementary proof in [14]. Another proof was found in 2020 by Lawrence and Venkatesh [52], using p-adic Hodge theory.

However, all of the proofs of Faltings' theorem are not completely effective, meaning that they do not give an algorithm which is able to find all the rational points. Ironically, other methods (mostly older), which so far have failed to prove the Mordell conjecture in full generality, are the ones that have succeeded in determining $\mathcal{C}(\mathbb{Q})$ in many examples.

In this thesis, we will focus on a class of those methods, which rely heavily on the properties of $\mathbb{Q}_p$ and on functions defined over $\mathbb{Q}_p$, and are therefore called *p-adic methods*. The first ideas behind them were originally developed by Chabauty in 1941.

Chabauty [22] proved (Theorem 2.3) that the Mordell conjecture holds if there is an additional condition regarding the rank of an abelian variety over $\mathbb{Q}$ associated with the curve, called the *Jacobian variety*. Later, in 1985, Coleman [27] used Chabauty's ideas to prove (Theorem 2.17) that under similar hypotheses, we can find a bound for $\#\mathcal{C}(\mathbb{Q})$.

Together, those two theorems are at the base of the so-called *Chabauty-Coleman method* which is the main method that we will study in this thesis. We will also study some of its generalizations and variants, and we will also see how to apply those methods to explicitely find rational solutions of Diophantine equations.

Acknowledgments

Vorrei ringraziare innanzitutto il prof. Matteo Longo per essere stato il relatore di questa tesi. Grazie per la sua pazienza e per tutti i suggerimenti e il supporto che mi ha dato, ma soprattutto per essere stato un punto di riferimento e una fonte di sostegno in tutti questi mesi.

Questi due anni sono stati sicuramente difficili per tutti e sono certo che sarebbero stati molto diversi se non avessi avuto tutti i miei amici a sopportarmi. Un ringraziamento speciale va quindi a Stefano, Emiliano, Federico e Lorenzo per tutte le serate passate a ridere al bar; a tutti i miei amici rimasti a Tor Vergata per tutti i giochi da tavolo che mi avete fatto provare; a Wiktor perché, sebbene fossimo lontani, le nostre discussioni matematiche (e non) non si sono mai fermate. Grazie anche a tutti quelli che ho incontrato a Padova, perché i (pochi) mesi che abbiamo passato insieme sono stati bellissimi.

Infine vorrei ringraziare la mia famiglia, per tutto il loro supporto e incoraggiamento durante i miei studi. Senza di loro non sarei la persona che sono ora.

Contents

1 Review of algebraic geometry **1**
- 1.1 Differentials . . . 2
- 1.2 Divisors and Riemann-Roch . . . 5
- 1.3 Abelian varieties and Jacobians . . . 9

2 Chabauty-Coleman theory **12**
- 2.1 Chabauty's theorem . . . 12
- 2.2 Coleman integration . . . 15
  - 2.2.1 Integration on Jacobians . . . 15
  - 2.2.2 An alternative proof of theorem 2.3 . . . 17
- 2.3 Coleman's theorem . . . 19
  - 2.3.1 Stoll's refinement of Coleman's theorem . . . 22
  - 2.3.2 Curves with sharp Coleman's bound . . . 27

3 Computational methods **30**
- 3.1 Construction of Coleman integrals in the rigid setting . . . 32
- 3.2 Algorithms for Coleman integrals . . . 40

4 Generalizations **56**
- 4.1 Elliptic Chabauty . . . 56
  - 4.1.1 How to apply Elliptic Chabauty . . . 59
  - 4.1.2 An explicit example . . . 64
- 4.2 Non-abelian Chabauty . . . 69
  - 4.2.1 Quadratic Chabauty . . . 72

5 Applications to Diophantine equations **74**
- 5.1 A question about triangles . . . 74
- 5.2 A challenge from Serre . . . 77
- 5.3 Generalized Fermat equations . . . 84

A The Mordell-Weil sieve **93**

Chapter 1

Review of algebraic geometry

This thesis will focus only on curves, i.e. varieties of dimension one, so in this section we will only talk about curves, even though many of the following arguments could be generalized to arbitrary varieties. For simplicity, we will mainly work on algebraically closed fields K but, again, most of what we will say can be generalized to more general fields (in particular we only need K to be perfect).

Let C/K be a curve. Since it has dimension 1, its function field $K(C)$ has transcendence degree one. Therefore $K(C)$ is algebraic over any subfield $K(x)$ generated by a nonconstant function $x \in k(C)$. It follows that there are two nonconstant functions on C, $x, y \in K(C)$, satisfying an algebraic relation $P(x, y) = O$ such that $K(C) = K(x, y)$. Let $C_0 \subseteq \mathbb{A}^2$ be the affine plane curve defined by P, and let $C_1 \subseteq \mathbb{P}^2$ be the projective plane curve defined by the homogenized polynomial

$$P_{hom}(X, Y, Z) = Z^{\deg P} P\left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

Clearly, C is birational to both C_0 and C_1.

We will say that any curve birational to C is a *model* of C, so that any curve has a plane affine model and a plane projective model. However, we can show that these model cannot be always smooth. Despite this, we have the following theorem.

Theorem 1.1. *Any algebraic curve is birational to a unique (up to isomorphism) smooth projective curve.*

Proof. See [41, Theorem 7.5.3] or [44, Corollary I.6.11].The idea is to repeatedly blow up the singular points and show that after a finite number of steps the resulting curve is smooth. □

In light of this result, in the following we will always assume (unless explicitly stated) that all the curves are smooth and projective.

1.1 Differentials

Definition 1.2. Let K be a field, R be a ring containing K and M be a R-module. A *derivation* of R into M over K is a K-linear map $D : R \to M$ such that

$$D(xy) = xD(y) + yD(x)$$

for all $x, y \in R$.

Remark 1.3. Notice that we must have $D(\lambda) = 0$ for every $\lambda \in K$, since

$$D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = D(1) + D(1)$$

so $D(1) = 0$ and therefore $D(\lambda) = \lambda D(1) = 0$ by the K-linearity. This also implies that the K-linearity in the definition above is equivalent to say that D is identically 0 on K.

By using properties of polynomials, we easily see that such a map acts on polynomials $K[X_1, \ldots, X_n]$ as follows:

$$D(P(x_1, \ldots, x_n)) = \sum_{i=0}^{n} \frac{\partial P}{\partial X_i}(x_1, \ldots, x_n) D(x_i)$$

for any $x_1, \ldots, x_n \in R$.

Proposition 1.4. *Let R be a domain with field of fractions k and let M be a vector space over k. Then a derivation $D : R \to M$ extends uniquely to a derivation $\widetilde{D} : K \to M$.*

Proof. Let $z = x/y \in k$ with $x, y \in R$. Then, if such a $\widetilde{D}$ exists, we must have:

$$D(x) = \widetilde{D}(x) = \widetilde{D}(yz) = y\widetilde{D}(z) + z\widetilde{D}(y) = y\widetilde{D}(z) + zD(y)$$

since D and $\widetilde{D}$ coincide on R. Therefore we must have:

$$\widetilde{D}(z) = \frac{1}{y}(D(x) - zD(y))$$

So we can take this as a definition of $\widetilde{D}$, proving existence and uniqueness. In order to see that this equation actually defines a derivation, we need to check that this map is K-linear (which is trivial) and that it satisfies the Leibniz rule:

$$\begin{aligned}
\widetilde{D}\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= \frac{1}{bd}\left(D(ac) - \frac{ac}{bd}D(bd)\right) \\
&= \frac{1}{bd}\left(aD(c) + cD(a) - \frac{ac}{bd}(bD(d) + dD(b))\right) \\
&= \frac{1}{bd}\left(cD(a) - \frac{ac}{b}D(b) + aD(c) - \frac{ac}{d}D(d)\right) \\
&= \frac{c}{d} \cdot \frac{1}{b}\left(D(a) - \frac{a}{b}D(b)\right) + \frac{a}{b} \cdot \frac{1}{d}\left(D(c) - \frac{c}{d}D(d)\right) \\
&= \frac{c}{d}\widetilde{D}\left(\frac{a}{b}\right) + \frac{a}{b}\widetilde{D}\left(\frac{c}{d}\right)
\end{aligned}$$

Hence this is indeed a derivation. Finally, we check that $\widetilde{D}$ actually extends D. Using remark 1.3 and writing $x = \frac{x}{1}$ shows that $\widetilde{D}$ agrees with D on R, as:

$$\widetilde{D}(x) = \widetilde{D}\left(\frac{x}{1}\right) = D(x) - xD(1) = D(x)$$

□

Now, let F be a free R-module with generating set R. That is, an element in F is a formal (finite) sum of elements in R with coefficients in R and with scalar multiplication given by multiplication in R.

Let N be the submodule of F generated by

$$(x+y)-x-y, \qquad (\lambda x)-\lambda\cdot x, \qquad (xy)-x\cdot y-y\cdot x$$

where $\lambda \in R$ is just a scalar, while $x, y, x+y, xy, \lambda x$ must be considered as elements of F, and $\cdot$ represents scalar multiplication in F (so that the expression $x \cdot y$ means that we are multiplying $y \in F$ by the scalar $x \in R$).

Definition 1.5. Define $\Omega^1_{R/K} = F/N$. We can call dx the image of x under the quotient map (take this as the definition of the map d). We will call this set *the module of differentials of R over K*.

Remark 1.6. The map d is a derivation. In fact, for all $x, y \in R \subseteq F$ and $\lambda \in R$ we have:

$$d(x+y) = (x+y) \pmod N = (x \pmod N) + (y \pmod N) = dx + dy$$

$$d(\lambda x) = (\lambda x) \pmod N = \lambda(x \pmod N) = \lambda dx$$

$$d(xy) = (xy) \pmod N = y(x \pmod N) + x(y \pmod N) = ydx + xdy$$

using the definition of N. So $d : F \to \Omega^1_{R/K} = F/N$ is an R-linear map which satisfies the Leibniz rule and we have

$$d\left(\sum \lambda_i x_i\right) = \sum \lambda_i dx_i$$

We also have the following Proposition, which follows directly from the action of a derivation on a polynomial in $K[x_1, \ldots, x_n]$ described earlier.

Proposition 1.7. *Suppose that $x_1, \ldots, x_n \in R$ are generators for R as a free K-module, then $\Omega^1_{R/K}$ is generated by the elements $dx_1, \ldots, dx_n$ as an R-module.*

Now, we can define the module of differentials for a curve.

Definition 1.8. If X is the nonsingular model of a projective curve C over K, then we define the *space of differentials of C over K* as the module $\Omega^1_{K(X)/K}$, where $K(X)$ is the function field of X (if the field is trivial from the context we will write $\Omega^1(X)$). These are analogous to the 1-forms in the case where $K = \mathbb{C}$.

Until now, we have defined differentials only algebraically, but we can take a more geometrical approach.

Let P be a point on a variety V.

Definition 1.9. The *local ring of V at P* is the ring $\mathcal{O}_{P,V}$ (or $\mathcal{O}_V$ if there is no confusion) of functions $f : V \to \overline{K}$ which are regular at P, where we identify two such functions if they coincide on an open neighborhood of P. We define $\mathcal{M}_{P,V}$ to be the (unique) maximal ideal of $\mathcal{O}_{P,V}$ which consists of the functions which vanish at P.

Definition 1.10. The *tangent space to V at P* (denoted as $\mathrm{Tan}_P(V)$) is the dual of the $\overline{K}$-vector space $\mathcal{M}_{P,V}/\mathcal{M}_{P,V}^2$. The $\overline{K}$-vector space $\mathcal{M}_{P,V}/\mathcal{M}_{P,V}^2$ is also called the *cotangent space to V at P*.

It can be proved that both the tangent and the cotangent space have finite dimension as $\overline{K}$-vector spaces. Moreover, we have the following theorem.

Theorem 1.11. *We have that* $\dim(\mathrm{Tan}_P(V)) \geq \dim(V)$ *for all* $P \in V$. *Furthermore, there exists a nonempty open subset* $U \subseteq V$ *such that* $\dim(\mathrm{Tan}_P(V)) = \dim(V)$ *for all* $P \in U$.

Proof. See [44, Proposition I.5.2A and Theorem I.5.3] or [65, Theorem II.2.3]. □

Definition 1.12. A point P on a variety V is called *singular* if $\dim(\mathrm{Tan}_P(V)) > \dim(V)$ and *nonsingular* (or *smooth*) if $\dim(\mathrm{Tan}_P(V)) = \dim(V)$. The variety V is called *nonsingular* (or *smooth*) if all of its points are nonsingular.

Now consider a rational map $f : V \to W$ which is regular at P and let $Q = f(P)$. It is known (see [46, Theorem A.1.2.5]) that f induces an homomorphism of local rings $f^* : \mathcal{O}_{Q,W} \to \mathcal{O}_{P,V}$ and hence a $\overline{K}$-linear map

$$f^* : \mathcal{M}_{Q,W}/\mathcal{M}_{Q,W}^2 \to \mathcal{M}_{P,V}/\mathcal{M}_{P,V}^2$$

Definition 1.13. The *tangent map* $df(P) : \mathrm{Tan}_P(V) \to \mathrm{Tan}_Q(W)$ is the transpose of the map $f^* : \mathcal{M}_{Q,W}/\mathcal{M}_{Q,W}^2 \to \mathcal{M}_{P,V}/\mathcal{M}_{P,V}^2$.

Now take a function $f \in K(V)^\times$, for any point x in its domain we have a tangent map $df(x) : \mathrm{Tan}_x(V) \to \mathrm{Tan}_{f(x)}(\mathbb{A}^1(K)) = K$. This implies that $df(x)$ is a linear form on $\mathrm{Tan}_x(V)$ and we have the identities

$$d(f+g) = df + dg \qquad \text{and} \qquad d(fg) = f\,dg + g\,df$$

where all the operations on f, g are defined pointwise.

This means that we can see df as a map that sends each point x in which f is defined to a linear form on $\mathrm{Tan}_x(V)$ (i.e. a cotangent vector). We call such a map an *abstract differential form*.

Definition 1.14. A *regular differential 1-form* on a variety V is an abstract differential form ω such that for all $x \in V$ there is a neighborhood U of x and regular functions $f_i, g_i \in \mathcal{O}(U)$ such that $\omega = \sum f_i dg_i$ on U. We denote this set as $\Omega^1[V]$.

Definition 1.15. Let $U, U' \subseteq V$ two open subsets of V and let $\omega \in \Omega^1[U], \omega' \in \Omega^1[U']$. We define an equivalence relation on the pairs (ω, U) as follows:

$$(\omega, U) \sim (\omega', U') \iff \omega \equiv \omega' \text{ on } U \cap U'$$

An equivalence class under this relation is called a *rational differential 1-form* on V. The set of all rational differential 1-forms on V is denoted by $\Omega^1(V)$.

Clearly, $\Omega^1[V]$ is a K-vector space and $\Omega^1(V)$ is $K(V)$-vector space.

Theorem 1.16. *Let V be a smooth variety, then the dimension of $\Omega^1(V)$ as a $K(V)$-vector space is equal to* $\dim(V)$.

Proof. This is a special case of Theorem III.3.19 from [65]. □

In particular, if C/K is a curve, then $\Omega^1(C)$ is a 1-dimensional $K(C)$-vector space, and therefore a general differential can be written as $\omega = fdg$ where $f, g \in K(X)$ with $dg \neq 0$. If we fix g this representation is unique.

Moreover, if we have $\omega, \omega' \in \Omega^1(C)$ with $\omega' \neq 0$, then there is a unique $f \in K(C)$ such that $\omega = f\omega'$.

Definition 1.17. Let $0 \neq \omega \in \Omega^1(C)$ and $P \in C(K)$. Moreover, let $t \in K(C)$ be a uniformizer at P. Then we can define $v_P(\omega)$ as $v_P(\omega/dt)$, where in the second case the valuation is the P-adic valuation on the field $K(C)$. This valuation is nonzero for only finitely many points $P \in C(\overline{K})$.

If $v_P(\omega) \geq 0$ then ω is regular at P and ω is said to be regular if it is regular at all points $P \in C(\overline{K})$. Regular differentials are also called *differentials of the first kind*.

A *differential of the second kind* has residue zero at all points $P \in C(\overline{K})$.

A *differential of the third kind* has at most a simple pole at all points $P \in C(\overline{K})$ (and integer residues there in some references).

1.2 Divisors and Riemann-Roch

Consider a nonsingular, irreducible and projective curve C.

Definition 1.18. The *group of divisors on C* is the free abelian group $\mathrm{Div}(C)$ generated by its $\overline{K}$-rational points[1]. Alternatively, a *divisor* on C is a formal finite sum

$$D = \sum n_i P_i$$

of points $P_i \in C(\overline{K})$ with coefficients $n_i \in \mathbb{Z}$. If $D_1 = \sum n_i P_i$ and $D_2 = \sum m_i P_i$, then we will write $D_1 + D_2$ to denote the divisor $\sum (n_i + m_i) P_i$.

Remark 1.19. The divisors we just defined are called *Weil divisors*. There is another way to define divisors, due to Cartier, but for smooth curves the two definition are equivalent, so we will only use the one above.

Definition 1.20. The support of the divisor $D = \sum n_i P_i$ is the set of points P_i such that $n_i \neq 0$. This subset of C is denoted by $\mathrm{supp}(D)$.

Definition 1.21. The degree of a divisor $D = \sum n_i P_i$ is the integer $\deg(D) = \sum n_i$. Clearly $\deg(D_1 + D_2) = \deg(D_1) + \deg(D_2)$. So we can interpret $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ as a group homomorphism; its kernel we be denoted by $\mathrm{Div}^0(C)$.

[1] For this definition we need that C is a curve. For general varieties we use closed subvarieties of codimension 1 instead of points.

Definition 1.22. If all the $n_i \geq 0$, then the divisor $D = \sum n_i P_i$ is called *effective* (or *positive*) and we will write $D \geq 0$. We will write $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

So far, we have only used $\overline{K}$-rational points of C, but this is not suitable to study the arithmetic of C over K. So we need to know what it means for a divisor to be defined over K.

Definition 1.23. The group $\mathrm{Gal}\left(\overline{K}/K\right)$ acts on $C(\overline{K})$ in a natural way, hence it also acts on $\mathrm{Div}(C)$. The fixed points for this action are called *K-rational divisors* and they form a subgroup, which we denote by $\mathrm{Div}_K(C)$.

Remark 1.24. If $P_1, \ldots, P_r \in C(K)$, then clearly $D = \sum n_i P_i \in \mathrm{Div}_K(C)$, since $\mathrm{Gal}\left(\overline{K}/K\right)$ acts trivially on the support. However, a divisor can be K-rational even if the points in its support are not. For example, on the curve $C/\mathbb{Q} : y^2 = x^2 + 1$, the divisor $D = (i, 0) + (-i, 0)$ is $\mathbb{Q}$-rational, but $(\pm i, 0) \notin C(\mathbb{Q})$.

Recall that for any $f \in K(C)^\times$, $v_P(f)$ denotes the order of P as a zero or a pole of f. Then we have the following lemma.

Lemma 1.25. *The valuation function $v_P : K(C)^\times \to \mathbb{Z}$ has the following properties:*

- *$v_P(fg) = v_P(f) + v_P(g)$ for all $f, g \in K(C)^\times$.*
- *Fix $f \in K(C)^\times$. Then there are only finitely many points P such that $v_P(f) \neq 0$.*
- *Let $f \in K(C)^\times$. Then $v_P(f) \geq 0$ if and only if $f \in \mathcal{O}_{P,C}$. Similarly, $v_P(f) = 0$ if and only if $f \in \mathcal{O}_{P,C}^\times$.*
- *If C is projective and $f \in K(C)^\times$, then the following are equivalent:*
  - *$v_P(f) \geq 0$ for every P.*
  - *$v_P(f) = 0$ for every P.*
  - *$f \in K^\times$.*

This lemma allows us to define the divisor of a function.

Definition 1.26. Let $f \in K(C)^\times$ be a rational function on C. The divisor of f is the divisor

$$\mathrm{div}(f) = \sum_{P \in C} v_P(f) P \in \mathrm{Div}(C)$$

A divisor is said to be *principal* if it is the divisor of a function. Note that since a rational function has the same number of zeros and poles (counting the zeros/poles at the point at infinity), a principal divisor will always have degree 0.

Definition 1.27. Two divisors $D_1, D_2 \in \mathrm{Div}(C)$ are said to be *linearly equivalent*, denoted by $D_1 \sim D_2$, if their difference is a principal divisor.

Remark 1.28. Clearly, if $f, g \in K(C)^\times$, then:

$$\mathrm{div}(f) = \mathrm{div}(g) \iff f = \lambda g$$

for some $\lambda \in K^\times$.

Proposition 1.29. *Linear equivalence of divisors is an equivalence relation.*

Proof. Reflexivity is trivial, as we can write D as the sum of itself plus the divisor of the constant function 1 which has no zeros nor poles.

Symmetry is also trivial, because if we have $D_1 \sim D_2$, so that $D_1 = D_2 + \mathrm{div}(f)$, then $D_2 = D_1 - \mathrm{div}(f)$, but $-\mathrm{div}(f) = \mathrm{div}(1/f)$.

For transitivity, let D_1, D_2, D_3 be divisors such that $D_1 \sim D_2$ and $D_2 \sim D_3$. Equivalently,

$$D_1 = D_2 + \mathrm{div}(f) \qquad \text{and} \qquad D_2 = D_3 + \mathrm{div}(g)$$

for some $f, g \in K(C)^\times$. Then we have:

$$D_1 = D_2 + \mathrm{div}(f) = D_3 + \mathrm{div}(f) + \mathrm{div}(g) = D_3 + \mathrm{div}(f \cdot g)$$

Hence linear equivalence is an equivalence relation. □

Remark 1.30. Clearly $D \sim 0$ if and only if D is principal and, since the degree of a divisor is an additive function, we also have that linearly equivalent divisors have the same degree.

It is easy to prove that the principal divisors form a subgroup of $\mathrm{Div}(C)$, which we will denote by $\mathrm{Princ}(C)$.

Definition 1.31. We define the *Picard group* of C as the quotient

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Princ}(C)$$

and

$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Princ}(C)$$

Equivalently, $\mathrm{Pic}(C)$ is the set of divisors modulo linear equivalence. We denote by $[D]$ the class of the divisor D in $\mathrm{Pic}(C)$.

Definition 1.32. Let D be a divisor of C. We define:

$$L(D) = \left\{ f \in K(C)^\times : \mathrm{div}(f) + D \geq 0 \right\} \cup \{0\}$$

This is a K-vector space whose dimension will be denoted by $l(D)$.

Proposition 1.33. *If $D_1 \leq D_2$ then $L(D_1) \subseteq L(D_2)$ and*

$$dim(L(D_2)/L(D_1)) \leq deg(D_2 - D_1)$$

Proof. We can write $D_2 = D_1 + \sum_{i=0}^{k} P_i$ for some $k \in \mathbb{N}$ (where the P_i are not necessarily distinct). Thus, it is obvious that if $f \in L(D_1)$ then $f \in L\left(D_1 + \sum_{i=0}^{k} P_i\right)$ by definition. So we've proven the first part of the statement.

We'll omit the proof of the second which involves a few more technical definitions (see [41, Chapter 8]). □

Lemma 1.34. $L(D) = 0$ *if* $\deg(D) < 0$.

Proof. Recall that $\deg(\mathrm{div}(f)) = 0$ for any $f \in K(C)^\times$, so if $\deg(D) < 0$, then $\deg(\mathrm{div}(f)+D) = \deg(\mathrm{div}(f))+\deg(D) = \deg(D) < 0$ and therefore we cannot have $\mathrm{div}(f)+D \geq 0$. This means that there are no nonzero functions in $L(D)$. □

Lemma 1.35.
- $L(0) = K$
- $K \subseteq L(D)$ *if and only if* $D \geq 0$

Proof.
- As in the previous proof, we have $\deg(\mathrm{div}(f)) = 0$ for any $f \in K(C)^\times$. This means that either $f \in K$ is a constant or has a zero, and therefore also a pole. Thus the only rational functions in $L(0)$ must be the functions without zeros or poles, which are the constant functions. This proves that $L(0) = K$.
- If $D \geq 0$, then for every constant function $c \in K$ we have that $\mathrm{div}(c) + D = 0 + D = D \geq 0$, so all the constants are in $L(D)$. Conversely, if $K \subseteq L(D)$, then $0 \leq \mathrm{div}(1) + D = D$.

□

Proposition 1.36. $L(D)$ *is a finite dimensional* K*-vector space for all* D*. In particular, if* $\deg(D) \geq 0$*, then* $l(D) \leq \deg(D) + 1$.

Proof. Let $\deg(D) = n \geq 0$ (we already saw that if $n < 0$, then $L(D) = 0$). Then choose a $P \in C$ and consider the divisor $D - (n+1)P$. The degree of this divisor is $\deg(D) - (n+1) = -1$, so $L(D-(n+1)P) = 0$. By Proposition 1.33, we must have $\dim(L(D)/L(D-(n+1)P)) \leq n+1$, which implies that $l(D) = \dim(L(D)) \leq n+1$. □

Proposition 1.37. *If* $D_1 \sim D_2$ *then* $l(D_1) = l(D_2)$.

Proof. Since $D_1 \sim D_2$, we must have $D_1 = D_2 + \mathrm{div}(f)$ for some $f \in K(C)$. So we can define a linear map between $L(D_1)$ and $L(D_2)$ by sending g to fg. Clearly this is an isomorphism of vector spaces and since the vector spaces are finite dimensional their dimensions must be equal. □

We define the divisor of $\omega \in \Omega^1(C)$ as we did for functions

$$\mathrm{div}(\omega) = \sum_{P \in C} v_P(\omega) P \in \mathrm{Div}(C)$$

where $v_P(\omega)$ is the valuation defined in definition 1.17. Recall also that if $\omega, \omega' \in \Omega^1(C)$ with $\omega' \neq 0$, then there is a unique $f \in K(C)$ such that $\omega = f\omega'$. In particular, we must have

$$\mathrm{div}(\omega) - \mathrm{div}(\omega') = \mathrm{div}\left(\frac{\omega}{\omega'}\right) = \mathrm{div}(f)$$

This proves that all the divisors of differentials are linearly equivalent. We call any of those divisors a *canonical divisor*.

Theorem 1.38 (Riemann-Roch)**.** *Let C be a smooth projective curve and W be a canonical divisor on C. Then there exists an integer $g \geq 0$ such that for any divisor $D \in \mathrm{Div}(C)$:*

$$l(D) - l(W - D) = deg(D) + 1 - g$$

Proof. See [41, Section 8.6]. □

Definition 1.39. The integer g is called the *genus* of the smooth projective curve C. If C is not smooth or projective, then its genus is defined to be the genus of a smooth projective model of C.

Theorem 1.40. *Let C be a smooth projective plane curve of degree n. Then the genus of g of C is given by*

$$g = \frac{(n-1)(n-2)}{2}$$

If C has only ordinary singularities, its genus is given by

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in S} \frac{m_P(m_P - 1)}{2}$$

where S is the set of singular points and m_P is the multiplicity of C at P.

Proof. See Theorems A.4.2.6 and A.2.4.7. of [46]. □

1.3 Abelian varieties and Jacobians

Definition 1.41. An *algebraic group* over K is a variety G, defined over K, with a marked point $e \in G(K)$ and morphisms $m : G \times G \to G$, $i : G \to G$ satisfying the axioms of a group law:

- $m(e, x) = m(x, e) = x$.
- $m(i(x), x) = m(x, i(x)) = e$.
- $m(m(x, y), z) = m(x, m(y, z))$.

Using this definition, we can easily prove that for any $x \in G$, the right and left translation maps

$$\begin{aligned} R_x : G &\longrightarrow G & L_x : G &\longrightarrow G \\ g &\longmapsto m(x, g) & g &\longmapsto m(g, x) \end{aligned}$$

are isomorphisms. We can use this information to prove the following theorem.

Theorem 1.42. *Algebraic groups are smooth varieties.*

Proof. For any $g_1, g_2 \in G$, we define $h = m(g_2, i(g_1))$. Then

$$R_h(g_1) = m(h, g_1) = m\big(m(g_2, i(g_1)), g_1\big) = m\big(g_2, m(i(g_1), g_1)\big) = m(g_2, e) = g_2$$

This proves that if there exists a nonsingular point $g \in G$, then for every $x \in G$ there exists $h \in G$ such that $R_h(g) = x$. However, the property that a point is singular is invariant under isomorphism, which implies that x is singular, and therefore so are all the points of G. But this contradicts the fact that the singular points of any algebraic variety form a proper closed subvariety. Therefore G cannot have singular points. □

Example 1.43. The *additive group* $\mathbb{G}_a$ is the variety $\mathbb{A}^1_K$ with the group law given by addition

$$\begin{aligned} m : \mathbb{G}_a \times \mathbb{G}_a &\longrightarrow \mathbb{G}_a \\ (x, y) &\longmapsto x + y \end{aligned}$$

Example 1.44. The *multiplicative group* $\mathbb{G}_m$ is the variety $\mathbb{A}^1_K \setminus \{0\}$ with the group law given by multiplication

$$\begin{aligned} m : \mathbb{G}_m \times \mathbb{G}_m &\longrightarrow \mathbb{G}_m \\ (x, y) &\longmapsto xy \end{aligned}$$

Example 1.45. The *general linear group* GL_n is the group of $n \times n$ invertible matrices with the group law given by matrix multiplication. Note that although GL_n is naturally defined as the quasi-projective variety

$$\mathrm{GL}_n = \{(x_{ij}) \in \mathbb{A}^{n^2} : \det(x_{ij}) \neq 0\}$$

it is actually an affine variety

$$\mathrm{GL}_n = \{(x_{ij}, t) \in \mathbb{A}^{n^2} \times \mathbb{A}^1 : t \det(x_{ij}) = 1\}$$

It is known that every algebraic group is a subgroup of GL_n for some n.

Another family of examples of algebraic groups is given by elliptic curves with the usual group law. The following definition generalize this last example.

Definition 1.46. An *abelian variety* is a projective variety that is also an algebraic group.

Notice that it is not immediately clear that an abelian variety must an abelian group. We will need a few result to prove this.

Lemma 1.47 (Rigidity lemma)**.** *Let X be a projective variety, and Y, Z be generic varieties. Let $f : X \times Y \to Z$ be a morphism. Suppose that there is a point $y_0 \in Y$ such that f is constant on $X \times \{y_0\}$. Then f is constant on every slice $X \times \{y\}$. If f is also constant on some slice $\{x_0\} \times Y$, then f is a constant function on all of $X \times Y$.*

Proof. We will only prove the first part since the second follows immediately.

Since X is a projective variety, and projective varieties are proper (see [44, Theorem 11.4.9]), the projection map $p : X \times Y \to Y$ is closed. So if we take an affine neighborhood U of $z_0 = f(x, y_0)$ (because by assumption $f(x, y_0)$ does not depend on x), then the set $W = p(f^{-l}(Z \setminus U))$ is closed in Y. By hypothesis, $y_0 \notin W$ and thus $Y \setminus W$ is a dense open subset of Y. For any $y \notin W$, the projective variety $f(X \times \{y\})$ is contained in the affine open set U, hence is reduced to a point. □

Corollary 1.48. *Let $\phi : A \to B$ be a morphism between two abelian varieties. Then we can write ϕ as the composition of a translation and a homomorphism.*

Proof. Let e_A and e_B be the identity elements of A and B, respectively. Up to composing ϕ with a translation, we may assume that $\phi(e_A) = e_B$. Instead of writing $m_A(x, y)$ and $i_A(x)$, we will write xy and x^{-1} to denote the group law and the inverse, without mentioning the group we are working in, since it will be obvious. Consider the map

$$\begin{aligned} f : A \times A &\longrightarrow B \\ (x, y) &\longmapsto \phi(xy)\phi(y)^{-1}\phi(x)^{-1} \end{aligned}$$

Clearly,$f(\{e_A\} \times A) = \{e_B\}$ and $f(A \times \{e_A\}) = \{e_B\}$, so Lemma 1.47 implies that f is constant. Therefore $f(x, y) = f(e_A, e_A) = e_B$, implying that ϕ is a homomorphism. □

Lemma 1.49. *An abelian variety is a commutative algebraic group.*

Proof. The previous corollary states that the inversion morphism

$$i : A \to A, \qquad i(x) = x^{-1}$$

must be a homomorphism. Hence $i(xy) = i(x)i(y)$, so A is commutative. □

One of the most important theorems in the arithmetic theory of abelian varieties is the famous Mordell-Weil theorem.

Theorem 1.50 (Mordell-Weil)**.** *Let A be an abelian variety defined over a number field K. Then the group $A(K)$ of K-rational points is finitely generated, that is there exists $r \in \mathbb{N}$ (called rank of A/K) and a finite abelian group T such that*

$$A(K) \cong \mathbb{Z}^r \oplus T$$

Traditionally, the proof is divided into two parts. At first, one proves the following "weaker" result:

Theorem 1.51 (Weak Mordell-Weil)**.** *Let A be an abelian variety defined over a number field K and let $m \geq 2$ be an integer. Then the group $A(K)/mA(K)$ is finite.*

Then, one constructs a suitable height function and uses a descent argument to prove Theorem 1.50. For the details, see [46, Part C].

Finally, one of the most important examples of abelian varieties in this thesis will be the *Jacobian variety of a curve C*:

Theorem 1.52. *Let C/K be a smooth projective curve of genus $g \geq 1$. Then, there exists an abelian variety $J = Jac(C)$ defined over K, called* Jacobian variety *of C. The dimension of J is equal to g and it is equipped with an injection $j : C \hookrightarrow J$ (called the* Abel-Jacobi map*) which induces a group isomorphism between $J(\overline{K})$ and $Pic^0(C)$, when extended by linearity to* $\mathrm{Div}(C)$.

Remark 1.53. If $P_0 \in C(K)$ we can prove that the Abel-Jacobi map $j : C \hookrightarrow J$ is defined over K. In particular, we can define

$$\begin{aligned} j : C &\hookrightarrow J \\ P &\mapsto [P - P_0] \end{aligned}$$

Chapter 2

Chabauty-Coleman theory

Throughout this chapter $C/\mathbb{Q}$ will be a smooth, projective, and geometrically irreducible curve of genus $g \geq 2$ and J will be its Jacobian variety.

For simplicity, we will only work over $\mathbb{Q}$ and $\mathbb{Q}_p$, even though all the results of the chapter can be generalized over number fields K (see also [66]), using $K_{\mathfrak{p}}$ (for some finite place $\mathfrak{p}$ of K) instead of $\mathbb{Q}_p$.

2.1 Chabauty's theorem

Before stating and prove Chabauty's theorem, we want to recall some results about the structure of the p-adic Lie group $J(\mathbb{Q}_p)$.
Let $J_{\mathbb{Q}_p}$ be the base change from $\mathbb{Q}$ to $\mathbb{Q}_p$ of J. We will denote by $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ the g-dimensional $\mathbb{Q}_p$-vector space of regular differential 1-forms on $J_{\mathbb{Q}_p}$. Let $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$, then we can use the translational invariance of ω_J to prove that there exists an "antiderivative"

$$\begin{aligned} \eta_J : J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ Q &\mapsto \int_0^Q \omega_J \end{aligned}$$

that is uniquely characterized by the following two properties:

1. η_J is an homomorphism of abelian groups. In order to prove this, denote by $t_P : J \to J, P' \mapsto P+P'$ the translation by P, then its derivative $dt_P : T_0J \to T_PJ$ is an isomorphism. Therefore the dual spaces $(T_0J)^\vee$ and $(T_PJ)^\vee$ are isomorphic. So every 1-form ω_J can be written as $(dt_P)^*(v)$ for some element $v \in (T_0J)^\vee$ and we have $t_P^*\omega_J = \omega_J$, thus:

$$\eta_J(P+Q) = \eta_J(P)+\int_P^{P+Q} \omega_J = \eta_J(P)+\int_0^Q t_P^*\omega_J = \eta_J(P)+\int_0^Q \omega_J = \eta_J(P)+\eta_J(Q)$$

2. There exists an open subgroup U of $J(\mathbb{Q}_p)$ such that for every $Q \in U$, $\eta_J(Q) = \int_0^Q \omega_J$ can be computed by writing ω_J as a power series in the local coordinates, then

finding a formal primitive and computing it in Q. Notice that since the coefficients in the series expansion of ω_J grow at most geometrically, the formal primitive converges on every sufficiently small U (see [16, Section III.7.6] for more details).

Remark 2.1. We may choose U as the kernel of the reduction map $J(\mathbb{Q}_p) \twoheadrightarrow J(\mathbb{F}_p)$. If p is a prime of good reduction, then $J(\mathbb{F}_p)$ can be seen as the group of points with coordinates in $\mathbb{F}_p$ on the reduction, but in general $J(\mathbb{F}_p)$ should be seen as the group of $\mathbb{F}_p$-points on the special fiber of the Néron model of J.

Lemma 2.2. *There exists a neighborhood U of $0 \in J(\mathbb{Q}_p)$ which is isomorphic (as a p-adic analytic group) to $\mathbb{Z}_p^g$. More precisely, there are local coordinates $t_1, \ldots, t_g$ near 0 and power series $\lambda_1, \ldots, \lambda_g \in \mathbb{Z}_p[[t_1, \ldots, t_g]]$ convergent in U and such that for all $P, Q \in U$ we have $P = (t_1(P), \ldots, t_g(P))$, $Q = (t_1(Q), \ldots, t_g(Q))$ e*

$$\lambda_i(t_1(P+Q), \ldots, t_g(P+Q)) = \lambda_i(t_1(P), \ldots, t_g(P)) + \lambda_i(t_1(Q), \ldots, t_g(Q))$$

Proof. As $\dim(T_0 J) = \dim(J) = g$ we get a g-dimensional set of η_J's which, by the properties above are power series convergent in U. Now, we only need to choose a basis $\lambda_1, \ldots, \lambda_g$ (For more details see [53]). □

Theorem 2.3 (Chabauty, 1942 [22])**.** *Let $\mathcal{C}/\mathbb{Q}$ be a curve of genus $g \geq 2$ such that $r = \operatorname{rank}(J(\mathbb{Q})) < g$, then $\mathcal{C}(\mathbb{Q})$ is a finite set.*

Proof. Let $U, \lambda_1, \ldots, \lambda_g$ as in the lemma and let $P_1, \ldots, P_r \in J(\mathbb{Q})$ be generators for the free part of $J(\mathbb{Q})$. Up to multiplication by a suitable power of p we may assume that $P_i \in U$. Consider the vectors

$$v_i = (\lambda_1(P_i), \ldots, \lambda_g(P_i)) \in \mathbb{Z}_p^g$$

then the matrix $V \in \mathbb{Z}_p^{r \times g}$ whose rows are the vectors $v_1, \ldots, v_r$ must have rank at most $r < g$ and therefore the columns are linearly dependent. In other words, there are $a_1, \ldots, a_g \in \mathbb{Z}_p$ not all zero such that

$$\sum_{i=1}^{g} a_i \lambda_i(P_j) = 0$$

for every $j = 1, \ldots, r$. We can define the function $\lambda(t_1, \ldots, t_g) = \sum_{i=1}^{g} a_i \lambda_i$ which is clearly analytic on U. By construction we know that $\lambda(P_j) = 0$ and from the lemma we deduce that λ is linear on U, so that

$$\lambda\left(\sum_{j=1}^{r} n_j P_j\right) = \sum_{j=1}^{r} n_j \lambda(P_j) = 0 \qquad \forall n_j \in \mathbb{Z}$$

In particular we notice that if $Q \in J(\mathbb{Q})$ then $p^m Q \in U$ for a sufficiently large $m \in \mathbb{N}$, so $\lambda(Q) = \frac{1}{p^m}\lambda(p^m Q) = 0$.

Suppose by contradiction that $\mathcal{C}(\mathbb{Q})$ is infinite. Then $\mathcal{C}(\mathbb{Q}) \subseteq \mathcal{C}(\mathbb{Q}_p)$ is compact (since $\mathcal{C}$ is projective) and consequently there is a limit point $P_0 \in \mathcal{C}(\mathbb{Q}_p)$. So there is $P_1 \in \mathcal{C}(\mathbb{Q})$ such that $[P_1 - P_0] \in U$ and for every $P \in \mathcal{C}(\mathbb{Q})$ sufficiently close to P_0, we have $[P - P_0] \in U$. This implies that $[P - P_1] \in J(\mathbb{Q}) \cap U$ and therefore $\lambda(P - P_1) = 0$. However λ is an analytic function on U and $\mathcal{C}$ has dimension 1, so either the set of zeros in $\mathcal{C}$ must be 0 dimensional (and therefore is finite since $\mathcal{C}$ is compact) or the map $\mu : P \mapsto \lambda(P - P_1)$ is identically zero:

- If $\mu \not\equiv 0$, the we can find only a finite number of P's sufficiently close to P_0, but this contradicts the fact that P_0 is a limit point for $\mathcal{C}(\mathbb{Q})$.
- If $\mu \equiv 0$, then for all $P \in \mathcal{C}(\mathbb{Q})$, $P - P_1 \in U$. If $Q_1, \ldots, Q_g \in \mathcal{C}(\mathbb{Q}_p)$ are close to P_1 then
$$0 = \sum_{i=1}^{g} \lambda(Q_i - P_1) = \lambda\left(Q_1 + \ldots + Q_g - gP_1\right)$$
However the set $\{[Q_1 + \ldots + Q_g - gP_1] \mid Q_1, \ldots, Q_g \in \mathcal{C}(\mathbb{Q}_p)\}$ is open in $J(\mathbb{Q}_p)$ and this implies that $\lambda \equiv 0$, which is a contradiction.

□

Remark 2.4. Although we will only work with curves, the ideas behind the proof can be used to work even with more general projective varieties V, provided that there exists a morphism $f : V \to A$, with A an abelian variety such that

$$\dim(V) \leq \dim(A) - \operatorname{rank}(A(\mathbb{Q}))$$

and such that we have some knowledge on the rational points on the fibers of f.

This restriction on the fibers is quite restrictive and rules out many types of varieties (e.g. K3 surfaces, since they only have constant maps to abelian varieties), but there are some examples for which this generalization works well, like restriction of scalars of curves or symmetric powers of curves (see [74]).

For the sake of completeness we will state (but not prove) a slightly stronger result but we need a few other remarks.

We have a bilinear pairing:

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) &\to \mathbb{Q}_p \\ (Q, \omega_J) &\longmapsto \int_0^Q \omega_J \end{aligned}$$

and in particular, if we denote T the dual vector space of $H^0(J_{\mathbb{Q}_p}, \Omega^1)$, then such pairing can be written as a group homomorphism

$$\begin{aligned} \log : J(\mathbb{Q}_p) &\to T \\ Q &\mapsto \left(\omega_J \mapsto \int_0^Q \omega_J\right) \end{aligned}$$

One can prove that the tangent spaces in 0 of $J(\mathbb{Q}_p)$ and T (as p-adic Lie groups) can be identified with T, which implies that the derivative of $\log$ in 0 is the identity on T. This proves that $\log$ is also a local diffeomorphism.

So the closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ (with the p-adic topology) is an analytical subgroup of $J(\mathbb{Q}_p)$ and as such we compute its dimension as a p-adic manifold. We have the following result:

Lemma 2.5. *Let $r' := \dim \overline{J(\mathbb{Q})}$ and $r := \operatorname{rank}(J(\mathbb{Q}))$. Then $r' \leq r$.*

Proof. Since $\log$ is a local diffeomorphism, $r' = \dim \overline{J(\mathbb{Q})} = \dim \log\left(\overline{J(\mathbb{Q})}\right)$ and since $\log$ is continuous and $\overline{J(\mathbb{Q})}$ is compact

$$\log\left(\overline{J(\mathbb{Q})}\right) = \overline{\log\left(J(\mathbb{Q})\right)} \subseteq T \cong \mathbb{Q}_p^g$$

The closure of every subgroup of $\mathbb{Q}_p^g$ is simply its $\mathbb{Z}_p$-span, so:

$$\begin{aligned} r' = \dim \overline{J(\mathbb{Q})} = \dim \log\left(\overline{J(\mathbb{Q})}\right) = \dim \overline{\log\left(J(\mathbb{Q})\right)} = \dim(\mathbb{Z}_p \log(J(\mathbb{Q}))) = \\ = \operatorname{rank}_{\mathbb{Z}_p}(\mathbb{Z}_p \log(J(\mathbb{Q}))) \leq \operatorname{rank}_{\mathbb{Z}}(\log(J(\mathbb{Q}))) \leq \operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) = r \end{aligned}$$

□

Remark 2.6. One can prove that the kernel of $\log$ is finite and from this deduce that actually $\operatorname{rank}_{\mathbb{Z}}(\log(J(\mathbb{Q}))) = \operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q}))$. However, it's not always true that

$$\operatorname{rank}_{\mathbb{Z}_p}(\mathbb{Z}_p \log(J(\mathbb{Q}))) = \operatorname{rank}_{\mathbb{Z}}(\log(J(\mathbb{Q})))$$

because $\mathbb{Z}$-independent points on $\log(J(\mathbb{Q}))$ need not to be $\mathbb{Z}_p$-independent. For example, we always have $r' \leq \dim(J) = g$ but it could happen that $r > g$, so that $r' < r$.

Theorem 2.7. *Let $\mathcal{C}/\mathbb{Q}$ be a curve of genus $g \geq 2$ and r' as above. If $r' < g$, then $\mathcal{C}(\mathbb{Q})$ is a finite set.*

Remark 2.8. By Lemma 2.5 $r' < g$ is always true if $r < g$; however, in practice, computing r' is significantly more difficult than computing r (which is still not easy). So, when making computations, it is more common to use the first version of Chabauty's theorem rather than the one we just stated.

2.2 Coleman integration

2.2.1 Integration on Jacobians

We want to define an integration map

$$\begin{aligned} H^0(J, \Omega^1_J) \times J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ (\omega, P) &\mapsto \int^P \omega \end{aligned}$$

such that:

- It is $\mathbb{Q}_p$-linear in ω;
- It is additive in P, i.e.
$$\int^{P+Q} \omega = \int^{P} \omega + \int^{Q} \omega$$
- It is non-degenerate up to torsion, i.e. $\int^P \omega = 0$ for every $\omega \in H^0(J, \Omega^1_J)$ if and only if P has finite order.

Lemma 2.9. *Let $\mathrm{Cot}(J)$ be the cotangent space to J at 0. Then the evaluation map*

$$ev : H^0(J, \Omega^1_J) \to \mathrm{Cot}(J)$$
$$\omega \mapsto \omega(0)$$

is an isomorphism of vector spaces.

Proof. The map $J \to \mathrm{Cot}(J), P \mapsto t_P^* \omega$ is algebraic. Since J is a complete variety and $\mathrm{Cot}(J)$ is an affine variety, it must be constant. This proves that any differential form is translation invariant, so ev must be injective.

The map ev is also surjective since the two spaces have both dimension g. □

Lemma 2.10. *For every $\omega \in H^0(J, \Omega^1_J)$ here exists a unique analytic map $\lambda_\omega : J(\mathbb{Q}_p) \to \mathbb{Q}_p$ such that $d\lambda_\omega = \omega$, $\lambda_\omega(0) = 0$ and λ_ω is a group homomorphism.*

Proof. We have that $\omega = \sum_{i=1}^{g} F_i dz_i$ for some $F_i \in \mathbb{Q}_p[[z_1, \ldots, z_g]]$. Then by the p-adic Poincaré lemma, we can write $\omega = dG$, for some $G \in \mathbb{Q}_p[[z_1, \ldots, z_g]]$ such that $G(0) = 0$ (otherwise take $G - G(0)$) and G converges on some open ball B. By lemma 2.2 there are open subgroups of $J(\mathbb{Q}_p)$ isomorphic to $(p^i\mathbb{Z}_p)^g$ that form a basis of neighborhood around 0, so without loss of generality, we can assume that B is an open subgroup of $J(\mathbb{Q}_p)$. Since J is compact, we have that $N = [J(\mathbb{Q}_p) : B]$ is finite, and we define

$$\lambda_\omega(P) = \frac{1}{N} G(N \cdot P)$$

Notice that for every $P \in J(\mathbb{Q}_p)$, $N \cdot P \in B$ by definition of N, so λ_ω is well-defined.

Checking that $d\lambda_\omega = \omega$ is pretty easy, since it is true on B and therefore on J because of translation invariance. Clearly, $\lambda_\omega(0) = 0$ is also true by definition of G.

Then, we have to check that λ_ω is a group homomorphism. Define, for every $a, b \in B$:

$$\int_a^b \omega := \lambda_\omega(b) - \lambda_\omega(a)$$

then this "integral" satisfies all the formal properties of integration, by definition. Therefore we have, since B is a subgroup:

$$\lambda_\omega(a+b) = \int_0^{a+b} \omega = \int_0^a \omega + \int_a^{a+b} \omega = \int_0^a \omega + \int_0^b t_a^* \omega = \int_0^a \omega + \int_0^b \omega = \lambda_\omega(a) + \lambda_\omega(b)$$

from this, it follows easily that λ_ω is an homomorphism.

Finally, we have to show that λ_ω is unique. This is true because of the local uniqueness at 0 and because of the fact that λ_ω is an homomorphism. □

Definition 2.11. Define $\int^P \omega = \lambda_\omega(P)$, for every $P \in J(\mathbb{Q}_p)$

Proposition 2.12. *This definition satisfies the condition we required for the integration map at the start of the section.*

Proof.

- Let $\omega_1, \omega_2 \in H^0(J, \Omega^1_J)$ and $\lambda_{\omega_1}, \lambda_{\omega_2}$ be the two associated homomorphisms. Then we only need to prove that $\lambda_{\omega_1+\omega_2} = \lambda_{\omega_1} + \lambda_{\omega_2}$. Let $\lambda = \lambda_{\omega_1} + \lambda_{\omega_2}$, then $\lambda(0) = 0$, $d\lambda = d(\lambda_{\omega_1} + \lambda_{\omega_2}) = \omega_1 + \omega_2$ and λ is an homomorphism. So by uniqueness, $\lambda = \lambda_{\omega_1+\omega_2}$.

- The fact that $\lambda_\omega(P + Q) = \lambda_\omega(P) + \lambda_\omega(Q)$ is simply the fact that λ_ω is an homomorphism.

- Let $\mathrm{Tan}(J)$ be the tangent space at the origin of $J(\mathbb{Q}_p)$, then we have a map:

$$\begin{aligned} i : J(\mathbb{Q}_p) &\to \mathrm{Tan}(J) \\ P &\mapsto (\omega \mapsto \lambda_\omega(P)) \end{aligned}$$

  Clearly, i is linear. Moreover, the differential at 0 of i is the identity, since $d\lambda_\omega|_0 = \omega$, so i is locally injective by translational invariance. So i is a locally injective homomorphism and its kernel is finite, and thus $\ker(i) \leq J(\mathbb{Q}_p)_{tors}$.

  However, $\mathrm{Tan}(J)$ is torsion-free, so $i\left(J(\mathbb{Q}_p)_{tors}\right) = 0$, hence we have an injective map

$$J(\mathbb{Q}_p)/J(\mathbb{Q}_p)_{tors} \hookrightarrow \mathrm{Tan}(J)$$

  or, equivalently, a pairing

$$J(\mathbb{Q}_p)/J(\mathbb{Q}_p)_{tors} \times \mathrm{Tan}(J)^\vee \to \mathbb{Q}_p$$

  which is non-degenerate on the left. Identifying $\mathrm{Tan}(J)^\vee$ with $H^0(J, \Omega^1_J)$ concludes the proof.

□

2.2.2 An alternative proof of theorem 2.3

One can show ([56, Prop. 2.2]) that the Abel-Jacobi embedding $\iota : \mathcal{C} \hookrightarrow J$ induces an isomorphism of $\mathbb{Q}_p$-vector spaces

$$\widetilde{\iota} : H^0(J_{\mathbb{Q}_p}, \Omega^1) \to H^0(\mathcal{C}, \Omega^1)$$

Now suppose that $\widetilde{\iota}(\omega_J) = \omega$, then for every $P, Q \in \mathcal{C}(\mathbb{Q}_p)$ we can define

$$\int_P^Q \omega = \int_0^{[Q-P]} \omega_J = \eta_J\left([Q - P]\right)$$

This suggests the following result.

Lemma 2.13. *Let $\mathcal{C}/\mathbb{Q}_p$ be a curve with good reduction in p. Then for every pair of points $P, Q \in \mathcal{C}(\mathbb{Q}_p)$ and for every regular differential $\omega \in H^0(\mathcal{C}, \Omega^1_{\mathcal{C}}(\mathbb{Q}_p))$ we can define a p-adic integral*

$$\int_P^Q \omega \in \overline{\mathbb{Q}_p}$$

such that:

1. *The integral is $\mathbb{Q}_p$-linear in ω;*
2. *If P and Q have the same reduction $\overline{P} \in \mathcal{C}_{\mathbb{F}_p}(\mathbb{F}_p)$, then the integral (which is also called tiny integral) can be computed by writing $\omega = \omega(t)dt$, where t is a uniformizer at P which reduces to a uniformizer at $\overline{P}$ and $\omega(t) \in \mathbb{Q}_p[[t]]$, and then integrating (formally) term by term $\omega(t)$. This yields a power series $l(t)$ such that $dl(t) = \omega(t)dt$ and $l(0) = 0$. In that case $\int_P^Q \omega = l(t(Q))$. In particular that implies that $\int_P^P \omega = 0$;*
3. *For every $P, P', Q, Q' \in \mathcal{C}(\mathbb{Q}_p)$ we have*

$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega$$

   So we can define

$$\int_D \omega = \sum_{j=1}^{n} \int_{P_j}^{Q_j} \omega$$

   for every $D = \sum_{j=1}^{n} (Q_j - P_j) \in Div^0_{\mathcal{C}}(\mathbb{Q}_p)$;

4. *For a fixed $P_0 \in \mathcal{C}(\mathbb{Q}_p)$ and for every $\omega \neq 0$, the set of points $P \in \mathcal{C}(\mathbb{Q}_p)$ such that reduce to a fixed point $\mathcal{C}_{\mathbb{F}_p}(\mathbb{F}_p)$ and $\int_{P_0}^P \omega = 0$ is finite.*

Remark 2.14. The condition that the curve has good reduction in p is not necessary but simplifies the statement of the second property.

So we find a pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(\mathcal{C}, \Omega^1) &\to \mathbb{Q}_p \\ ([D], \omega) &\mapsto \langle [D], \omega \rangle = \int_D \omega \end{aligned} \tag{2.1}$$

which is additive in the first entry and $\mathbb{Q}_p$-linear in the second. In particular, if $P \in \mathcal{C}(\mathbb{Q}_p)$, then

$$\langle \iota(P), \omega \rangle = \int_{P_0}^P \omega$$

where

$$\begin{aligned} \iota : \mathcal{C} &\to J_{\mathcal{C}} \\ P &\mapsto [P - P_0] \end{aligned}$$

is the Abel-Jacobi map and $P_0 \in \mathcal{C}(\mathbb{Q}_p)$ is a fixed point.

This is sufficient to give an alternative proof of Chabauty's theorem.

Alternative proof of theorem 2.3. Let p be a prime of good reduction for $\mathcal{C}$ and define

$$A = \{\omega \in H^0(\mathcal{C}, \Omega^1) | \, \langle P, \omega \rangle = 0 \; \forall P \in J(\mathbb{Q})\}$$

which is a linear subspace of $H^0(\mathcal{C}, \Omega^1)$ and whose elements are called *annihilating differentials*. By endpoint additivity, ω is an annihilating differential if and only if $\langle P_i, \omega \rangle = 0$, where $P_1, \ldots, P_r$ are a basis for the free part of $J(\mathbb{Q})$. On the other hand, by the $\mathbb{Q}_p$-linearity of the argument, these r conditions are linear relations which describe the subspace A and therefore $\dim A \geq g - r > 0$ which implies that, in particular, we can find $0 \neq \omega \in A \neq \emptyset$.

If $\mathcal{C}(\mathbb{Q}) = \emptyset$ we are done, otherwise we choose $P_0 \in \mathcal{C}(\mathbb{Q})$ from which we can fix the Abel-Jacobi embedding $\iota : \mathcal{C} \to J_{\mathcal{C}}, \; P \mapsto [P - P_0]$. Since $\iota(P) \in J(\mathbb{Q})$ for every $P \in \mathcal{C}(\mathbb{Q})$, we get that $\int_{P_0}^{P} \omega = 0$ for every $P \in \mathcal{C}(\mathbb{Q})$.

However, every point of $\mathcal{C}(\mathbb{Q})$ reduces to unique point of $\overline{\mathcal{C}}(\mathbb{F}_p)$, which is a finite set, but for every point on the reduction there are only finitely many points in $\mathcal{C}(\mathbb{Q})$ such that $\int_{P_0}^{P} \omega = 0$, which implies that $\mathcal{C}(\mathbb{Q})$ is finite. □

2.3 Coleman's theorem

We already saw in the proof of Chabauty's theorem that we could (at least in theory) compute $\#\mathcal{C}(\mathbb{Q})$ by finding an annihilating differential ω and for every fixed $P_1 \in \mathcal{C}(\mathbb{F}_p)$, the number of points $P \in \mathcal{C}(\mathbb{Q})$ that reduce to P_1 and such that $\int_{P_0}^{P} \omega = 0$. However, this is not an easy thing to do, but the same idea works if we use $\mathcal{C}(\mathbb{Q}_p)$ instead of $\mathcal{C}(\mathbb{Q})$, even though usually $\mathcal{C}(\mathbb{Q}) \subsetneq \mathcal{C}(\mathbb{Q}_p)$ and thus we can only find an upper bound.

As a matter of fact, we can estimate the number of zeros of $\int_{P_0}^{z} \omega$ as a p-adic power series. Moreover, purely from a set-theoretic point of view, we can regard $\mathcal{C}(\mathbb{Q}_p)$ as a finite union of residue disks (i.e. the preimages in $\mathcal{C}(\mathbb{Q}_p)$ of points in $\mathcal{C}(\mathbb{F}_p)$ under the reduction map), so that in each disk $\int_{P_0}^{z} \omega$ has only a finite number of zeros.

In order to do this we have to bound the number of points of a p-adic power series.

Lemma 2.15. *Let*

$$0 \neq l(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbb{Q}_p \, [[t]]$$

such that $\lim_{n \to \infty} a_n = 0$ *(in the p-adic topology). Let* $v_0 = \min\{v_p(a_n)\}$ *and*

$$N = \max\{n \geq 0 | \, v_p(a_n) = v_0\}$$

Then, there exist a constant $c \in \mathbb{Q}_p^{\times}$*, a monic polynomial* $q(t) \in \mathbb{Z}_p \, [t]$ *of degree* N *and a power series*

$$h(t) = \sum_{n=0}^{\infty} b_n t^n \in 1 + pt\mathbb{Z}_p \, [[t]]$$

with $\lim_{n \to \infty} b_n = 0$*, such that*

$$l(t) = cq(t)h(t)$$

Proof. Up to collecting a suitable power of t we can assume that $a_0 \neq 0$. Moreover, after normalizing the coefficients by multiplying $l(t)$ by a_N^{-1}, we can also assume that $v_0 = 0$ and $a_N = 1$, so that $l(t) \in \mathbb{Z}_p[[t]]$. In that case, the condition that $\lim_{n\to\infty} a_n = 0$ implies that the image $l_m(t)$ of $l(t)$ in $(\mathbb{Z}/p^m\mathbb{Z})[[t]]$ is a polynomial for every $m \geq 1$.
We will proceed inductively by constructing, for every $m \geq 1$, some constants $c_m \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, some monic polynomials $q_m \in (\mathbb{Z}/p^m\mathbb{Z})[t]$ of degree N and polynomials $h_m \in (\mathbb{Z}/p^m\mathbb{Z})[t]$ with $h_m \equiv 1 \pmod{pt}$, such that

$$l_m(t) = c_m q_m(t) h_m(t)$$

and with the property that $(c_{m+1}, q_{m+1}, h_{m+1})$ reduces modulo p^m to (c_m, q_m, h_m). This will allow us to find (unique) c, q and h as in the statement such that

$$(c, q, h) \equiv (c_m, q_m, h_m) \pmod{p^m}$$

We start by setting $c_1 = 1$, $q_1(t) = l_1(t)$ and $h_1(t) = 1$. We can do this because

$$l_1(t) \equiv a_N t^N + \ldots + a_0 \pmod{p}$$

as for every $n > N$ we have that $v_p(a_n) > v_0 = 0$ and $a_N = 1$, hence $l_1(t)$ is a monic polynomial of degree N.

Now suppose that we already constructed c_m, q_m and h_m. Let $\widetilde{c}_{m+1}, \widetilde{q}_{m+1}, \widetilde{h}_{m+1}$ arbitrary lifts of c_m, q_m, h_m at suitable objects over $\mathbb{Z}/p^{m+1}\mathbb{Z}$ such that $\widetilde{q}_{m+1}(t)$ is a monic polynomial of degree N and $\widetilde{h}_{m+1}(t) \equiv 1 \pmod{pt}$. Then

$$l_{m+1} - \widetilde{c}_{m+1}\widetilde{q}_{m+1}(t)\widetilde{h}_{m+1}(t) = p^m d(t)$$

where $d(t) \in (\mathbb{Z}/p\mathbb{Z})[t]$. Consequently, we must have

$$c_{m+1} = \widetilde{c}_{m+1} + p^m \gamma$$

$$q_{m+1}(t) = \widetilde{q}_{m+1}(t) + p^m r(t)$$

$$h_{m+1}(t) = \widetilde{h}_{m+1}(t) + p^m k(t)$$

where $\gamma \in \mathbb{Z}/p\mathbb{Z}$, $r(t) \in (\mathbb{Z}/p\mathbb{Z})[t]$ has degree $< N$ and $k(t) \in (\mathbb{Z}/p\mathbb{Z})[t]$ is such that $k(0) = 0$.

However $l_{m+1} = c_{m+1} q_{m+1}(t) h_{m+1}(t)$ is equivalent to say that

$$d(t) = (\gamma + k(t)) l_1(t) + r(t)$$

Then, by dividing $d(t)$ by $l_1(t)$ in $(\mathbb{Z}/p\mathbb{Z})[t]$, we can uniquely find $\gamma, r(t)$ and $k(t)$ and therefore $c_{m+1}, q_{m+1}, h_{m+1}$ are uniquely determined, too. □

Now, we will apply this lemma to the study of zeros of p-adic power series.

Theorem 2.16 (Strassman). *Let $l(t) \in \mathbb{Q}_p[[t]]$ with formal derivative $l'(t) = w(t) \in \mathbb{Z}_p[[t]]$. If the reduction $\overline{w}(t) \in \mathbb{F}_p[[t]]$ can be written as $\overline{w}(t) = ut^M + \ldots$ with $u \in \mathbb{F}_p^\times$, then $l(t)$ converges on $p\mathbb{Z}_p$. If moreover, $M < p - 2$ then*

$$\#\{\tau \in \mathbb{Z}_p \,|\, l(\tau) = 0\} \leq M + 1$$

Proof. Write $l(t) = l_0 + l_1 t + \ldots \in \mathbb{Q}_p[[t]]$ and $w(t) = l'(t) = w_0 + w_1 t + \ldots \in \mathbb{Z}_p[[t]]$. Then

$$l_{n+1} = \frac{w_n}{n+1} \in \frac{1}{n+1}\mathbb{Z}_p$$

and since $v_p(n+1) = O(\log n)$, we have that

$$v_p(l_n) = v_p(w_{n-1}/n) \geq -c\log(n)$$

for some positive constant c and for every sufficiently large n. Let $\tau \in p\mathbb{Z}_p$, then $v_p(\tau) \geq 1$ and therefore

$$v_p(l_n\tau^n) \geq n - c\log(n) \to \infty$$

if $n \to \infty$. So $\lim_{n\to\infty} l_n\tau^n = 0$ and this implies that $l(\tau)$ converges.

Now, consider $l(pt) = l_0 + pl_1 t + p^2 l_2 t^2 + \ldots$; we want to show that, with the same notations as in the previous lemma, we have $N \leq M+1$. We have that

$$v_p(p^{M+1}l_{M+1}) = M + 1 + v_p(l_{M+1}) = M + 1 + v_p(w_M) - v_p(M+1) \leq M+1$$

since by hypothesis $\overline{w}(t) = ut^M + \ldots \in \mathbb{F}_p[[t]]$, with $u \in \mathbb{F}_p^\times$ and thus $v_p(w_n) = 0$.
For $n > M$ we get

$$v_p(p^{n+1}l_{n+1}) = n + 1 + v_p(l_{n+1}) = n + 1 + v_p(w_n) - v_p(n+1) \geq n + 1 - v_p(n+1)$$

since $w_n \in \mathbb{Z}_p$ implies $v_p(w_n) \geq 0$. So we only need to prove that $n - v_p(n+1) > M$ for every $n > M$.
This is clearly true if $v_p(n+1) = 0$. Otherwise, let $e = v_p(n+1)$, so that $p^e \mid (n+1)$ and, consequently, $n + 1 \geq p^e$. However, for $e = 1$ we have $p > M + 2 = M + e + 1$, by hypothesis, and if $e > 1$ then $p^e \geq p^{e-1} + 1 > (M + (e-1) + 1) + 1 = M + e + 1$ by induction. For this reason $n + 1 \geq p^e > M + e + 1$ and therefore $n - v_p(n+1) > M$ for every $n > M$.

This proves that $v_0 \leq M + 1$ and $N \leq M + 1$, so that the previous lemma allows us to write

$$l(t) = cq(t)h(t)$$

where $c \in \mathbb{Q}_p^\times$, $q \in \mathbb{Z}_p[[t]$ is a monic polynomial of degree N and $h(t) \in 1 + pt\mathbb{Z}_p[[t]]$. Then, for every $\tau \in \mathbb{Z}_p$, $h(\tau) \equiv 1 \pmod{p}$ and therefore $h(\tau) \neq 0$. Then

$$\#\{\tau \in \mathbb{Z}_p |\, l(\tau) = 0\} = \#\{\tau \in \mathbb{Z}_p |\, q(\tau) = 0\} \leq \deg(q) = N \leq M + 1$$

□

We are now ready to prove Coleman's theorem.

Theorem 2.17 (Coleman, 1985 [27]). *Let $\mathcal{C}/\mathbb{Q}$ be a curve of genus $g \geq 2$, with*

$$r = \operatorname{rank}(J(\mathbb{Q})) < g$$

Let $p > 2g$ be a prime of good reduction for $\mathcal{C}$. Then

$$\#\mathcal{C}(\mathbb{Q}) \leq \#\mathcal{C}(\mathbb{F}_p) + 2g - 2$$

Proof. If $\mathcal{C}(\mathbb{Q})$ is empty, the theorem is trivially true because

$$\#\mathcal{C}(\mathbb{F}_p) + 2g - 2 \geq 2 \cdot 2 - 2 = 2 \geq 0 = \#\mathcal{C}(\mathbb{Q})$$

So suppose instead that there exists $P_0 \in \mathcal{C}(\mathbb{Q})$ then, as in the alternative proof of theorem 2.3, we can prove the existence of an annihilating differential $\omega \in H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/\mathbb{Q}_p})$, i.e. such that

$$\int_{P_0}^{P} \omega = 0$$

for every $P \in \mathcal{C}(\mathbb{Q})$. Now fix a point $\overline{Q} \in \overline{\mathcal{C}}(\mathbb{F}_p)$ and lift it to $Q \in \mathcal{C}(\mathbb{Q}_p)$; we can choose a uniformizer $t \in \mathbb{Q}_p(\mathcal{C})^\times$ at Q such that t reduces to a uniformizer $\bar{t} \in \mathbb{F}_p(\overline{\mathcal{C}})^\times$ at $\overline{Q}$. Up to multiplication by a constant, we can assume that the reduction of ω, $\overline{\omega}$, is well-defined and non-zero, so that $\overline{\omega} \in H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/\mathbb{F}_p})$. Notice that the associated divisor to $\overline{\omega}$, $\mathrm{div}(\overline{\omega})$, is effective and has degree $2g-2$.
We define $v(\overline{Q}) = v_{\overline{Q}}(\overline{\omega})$ and we write $\omega(t) = w(t)dt$, with $w(t) \in \mathbb{Z}_p[[t]]$ (all the coefficients are in $\mathbb{Z}_p$ because we assumed that the reduction $\overline{\omega}$ is well-defined). Then

$$\overline{\omega}(t) = \overline{w}(\bar{t})d\bar{t} = \bar{t}^{v(\overline{Q})}(u_0 + u_1\bar{t} + \ldots)$$

Let $l(t) \in \mathbb{Q}_p[[t]]$ a formal primitive of $w(t)$, then we already saw that $\int_{P_0}^{P} \omega = l(t(P))$ for every $P \in \mathcal{C}(\mathbb{Q}_p)$ such that $\overline{P} = \overline{Q}$ (in this case $t(P) \in p\mathbb{Z}_p$) and we can apply theorem 2.16, which yields

$$\begin{aligned}
\#\mathcal{C}(\mathbb{Q}) &\leq \#\left\{P \in \mathcal{C}(\mathbb{Q}_p) : \int_{P_0}^{P} \omega = 0\right\} \\
&= \sum_{\overline{Q} \in \overline{\mathcal{C}}(\mathbb{F}_p)} \#\left\{P \in \mathcal{C}(\mathbb{Q}_p) : \overline{P} = \overline{Q}, \int_{P_0}^{P} \omega = 0\right\} \\
&\leq \sum_{\overline{Q} \in \overline{\mathcal{C}}(\mathbb{F}_p)} \big(v(\overline{Q}) + 1\big) \\
&= \sum_{\overline{Q} \in \overline{\mathcal{C}}(\mathbb{F}_p)} v(\overline{Q}) + \sum_{\overline{Q} \in \overline{\mathcal{C}}(\mathbb{F}_p)} 1 \\
&\leq \deg(\mathrm{div}(\omega)) + \#\overline{\mathcal{C}}(\mathbb{F}_p) \\
&= \#\overline{\mathcal{C}}(\mathbb{F}_p) + 2g - 2
\end{aligned}$$

□

2.3.1 Stoll's refinement of Coleman's theorem

In 2006, Stoll proved an improvement of Coleman's result. Even though it is possible to work over any number field, we continue to work only over $\mathbb{Q}$. For the general results over number fields we refer the reader to the original article [70].

First of all, we need some notation.
Let D be a $\overline{\mathbb{Q}}$-defined divisor on $\mathcal{C}$ and define $\Omega(D)$ as the $\overline{\mathbb{Q}}$-vector space of differentials ω on $\mathcal{C}$ such that $\mathrm{div}(\omega) \geq D$. Define also the function $f_{\mathcal{C}} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$

as

$$f_{\mathcal{C}}(r) = \max\{\deg(D) \mid D \geq 0,\ \dim \Omega(D) \geq g - r\}$$

Clearly, $f_{\mathcal{C}}(r) = \infty$ whenever $r \geq g$, otherwise we have the following result

Lemma 2.18. *1. If $0 \leq r < g$, then $r \leq f_{\mathcal{C}}(r) \leq 2r$;*

2. $f_{\mathcal{C}}(0) = 0$ and $f_{\mathcal{C}}(g-1) = 2g-2$;

3. $\mathcal{C}$ is an hyperelliptic curve if and only if $f_{\mathcal{C}}(1) = 2$;

4. If $\mathcal{C}$ is an hyperelliptic curve then $f_{\mathcal{C}}(r) = 2r$ for any $0 \leq r < g$;

5. If $\mathcal{C}$ is a smooth plane curve of degree n, then

$$f_{\mathcal{C}}(r) = r + \binom{n-a}{2} - 1$$

where

$$a = \max\left\{k : r + \binom{k}{2} < g = \binom{n-1}{2}\right\} = \left\lfloor \frac{1 + \sqrt{4n^2 - 12n + 9 - 8r}}{2} \right\rfloor$$

Proof. 1. Since $\dim \Omega(D) \geq g - \deg(D)$ for any effective divisor D, then $f_{\mathcal{C}}(r) \geq r$. For the opposite inequality, we use Riemann-Roch and the standard bound

$$\dim L(D) \ \leq\ 1 + \frac{1}{2}\ \deg(D)$$

for any divisor D such that $0 \leq \deg(D) \leq 2g$. This implies

$$g - r \leq \dim \Omega(D) = \dim L(D) - \deg(D) + g - 1 \leq g - \frac{1}{2}\deg(D)$$

and therefore $\deg(D) \leq 2r$.

2. Clearly $f_{\mathcal{C}}(0) = 0$. For the other equality, just take D equal to the canonical divisor.

3., 4. and 5. are well-known facts about hyperelliptic and plane curves (see [44]). □

We now need to consider $f_{\overline{\mathcal{C}}/\mathbb{F}_p}(r)$ for the reduction of $\mathcal{C}$ at a prime p of good reduction. It is possible that $f_{\overline{\mathcal{C}}/\mathbb{F}_p}(r) > f_{\mathcal{C}}(r)$ for some p and r (for an example see [35]). However, we have the following Proposition

Proposition 2.19. *There are at most a finite number of primes p of good reduction for $\mathcal{C}$ such that $f_{\overline{\mathcal{C}}/\mathbb{F}_p} \not\equiv f_{\mathcal{C}}$.*

Proof. See [70, Proposition 3.2.]. □

Define, for every $n \in \mathbb{Z}_{\geq 0}$:

$$\delta_p(n) = \max\{d \geq 0 | v_p(n+1) + d \leq v_p(n+d+1)\}$$

and for $s, r \geq 0$, let

$$\Delta_p(s,r) = \max\left\{\sum_{i=1}^{s} \delta_p(m_i) : \sum_{i=1}^{s} m_i \leq r, m_i \in \mathbb{Z}_{\geq 0}\right\}$$

Notice that Δ_p is obviously an increasing function in both arguments.

We need to bound δ_p and Δ_p from above. We will use the following two lemmas.

Lemma 2.20. *If $p \geq 3$, then $\delta_p(n) \leq \left\lfloor \frac{n}{p-2} \right\rfloor$. In particular if $n < p-2$, then $\delta_p(n) = 0$.*

Proof. If $\delta_p(n) = d$, then $v_p(n+d+1) \geq v_p(n+1) + d \geq d$. Therefore p^d divides $n+d+1$ and, in particular, $p^d \leq n+d+1$. Hence, we always have

$$\delta_p(n) \leq \max\{d \geq 0 | p^d \leq n+d+1\}$$

If we suppose further that $p \geq 3$, then it's easy to prove by induction that

$$p^d - d - 1 \geq (p-2)d$$

for any $d \geq 0$, thus

$$n \geq p^d - d - 1 \geq (p-2)d \Longrightarrow d \leq \frac{n}{p-2}$$

for every $d \geq 0$ such that $p^d \leq n+d+1$. □

Lemma 2.21. *If $p \geq 3$, then $\Delta_p(s,r) \leq \left\lfloor \frac{r}{p-2} \right\rfloor$. In particular if $r < p-2$, then $\Delta_p(s,r) = 0$.*

Proof. If $\sum_{i=1}^{s} m_i \leq r$, then

$$\sum_{i=1}^{s} \delta_p(m_i) \leq \sum_{i=1}^{s} \left\lfloor \frac{m_i}{p-2} \right\rfloor \leq \left\lfloor \frac{\sum_{i=1}^{s} m_i}{p-2} \right\rfloor \leq \left\lfloor \frac{r}{p-2} \right\rfloor$$

□

For any $P \in \overline{\mathcal{C}}(\overline{\mathbb{F}_p})$, we denote by $D_P \subseteq \mathcal{C}(\overline{\mathbb{Q}_p})$ the residue class of P, i.e. the preimage of P under the reduction map $\rho : \mathcal{C}(\overline{\mathbb{Q}_p}) \to \overline{\mathcal{C}}(\overline{\mathbb{F}_p})$, and we write $D_P(\mathbb{Q}_p) = D_P \cap \mathcal{C}(\mathbb{Q}_p)$.

Let $G = \{P \in J(\mathbb{Q}_p) | \, nP \in J(\mathbb{Q}) \text{ for some } n > 0\}$ and let

$$A = \{\omega \in H^0(\mathcal{C}, \Omega^1(\mathbb{Q}_p)) | \, \langle P, \omega \rangle = 0 \; \forall P \in J(\mathbb{Q})\}$$

as in the alternative proof of theorem 2.2. Then we already saw that $\dim A \geq g - r$, where $r = \mathrm{rank}(J(\mathbb{Q}))$. Notice that for every $P \in G$ and for every $\omega \in A$ we have that

$$\langle P, \omega \rangle = \frac{1}{n}\langle nP, \omega \rangle = 0$$

Define $X = \{P \in \mathcal{C}(\mathbb{Q}_p) | \, \iota(P) \in G\}$, where $\iota : \mathcal{C} \hookrightarrow J$ is a fixed Abel-Jacobi map, and notice that $\mathcal{C}(\mathbb{Q}) \cup i^{-1}(J(\mathbb{Q}_p)_{tors}) \subseteq X$. Let also $\overline{X}$ denote the image of X in $\overline{\mathcal{C}}(\mathbb{F}_p)$ under the reduction map.

Let $0 \neq \omega \in H^0(\mathcal{C}, \Omega^1(\mathbb{Q}_p))$, then, up to multiplication by a constant, we can assume that its reduction $\overline{\omega}$ is well-defined and not zero, so that $\overline{\omega} \in H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/\mathbb{F}_p})$. If $P \in \overline{\mathcal{C}}(\mathbb{F}_p)$ we denote by $n(\omega, P) = v_P(\overline{\omega})$ the order of vanishing of $\overline{\omega}$ in P. We also write $\nu(P) = \#(D_P \cap X)$.
Then we have the following Proposition.

Proposition 2.22. *Let $0 \neq \omega \in A$ and $P \in \overline{\mathcal{C}}(\mathbb{F}_p)$. Then*

$$\nu(P) \leq 1 + n(\omega, P) + \delta_p(n(\omega, P))$$

Proof. As before, we can assume that ω reduces to $\overline{\omega}$ and let $n = n(\omega, P)$. Choose an uniformizer t at a point in $D_P(\mathbb{Q}_p)$, so that

$$\overline{\omega} = (u\bar{t}^n + \text{higher order terms})d\bar{t}$$

with $u \in \mathbb{F}_p^\times$. But this implies that we can write

$$\omega = (a_0 + a_1 t + a_2 t^2 + \ldots)dt$$

where $a_0, a_1, \ldots, a_{n-1}$ have positive p-adic valuation and a_n is a p-adic unit. Define

$$L_\omega(T) = c + a_0 pT + \ldots + \frac{a_m}{m+1} p^{m+1} T^{m+1} + \ldots$$

and $\langle Q, \omega \rangle = l_\omega(Q) = L_\omega(T)$, where $t(Q) = pT$ and $T \in \mathbb{Z}_p$, for every $Q \in D_P(\mathbb{Q}_p)$. Then, by standard results on Newton polygons (see [43, Section 7.4]), l_ω has at most $1 + n + \delta_p(n)$ zeros in $D_P(\mathbb{Q}_p)$, since these zeros correspond to integral zeros of the power series L_ω.

Since $X \cap D_P$ is contained in this set of zeros (because for every $R \in X$, $\iota(R) \in G$, thus $\langle \iota(R), \omega \rangle = 0$), the claim follows. □

In light of the above, for every $\mathbb{Q}_p$-linear subspace $\Lambda \neq 0$ of $H^0(\mathcal{C}, \Omega^1(\mathbb{Q}_p))$, we define

$$n(\Lambda, P) = \min\{n(\omega, P) | \, 0 \neq \omega \in \Lambda\}$$

$$N(\Lambda, \mathcal{C}/\mathbb{Q}_p) = \sum_{P \in \overline{\mathcal{C}}(\mathbb{F}_p)} n(\Lambda, P)$$

We now give a general result.

Theorem 2.23. *Let $C/\mathbb{Q}_p$ be a smooth projective curve of genus g, and let $\Lambda \neq 0$ as above. If C has good reduction at p, then*

$$N(\Lambda, C/\mathbb{Q}_p) \leq f_{C/\mathbb{F}_p}(\operatorname{codim}\Lambda) \leq 2\operatorname{codim}\Lambda$$

Proof. Because of good reduction, there is a well-defined reduction map

$$\rho : \mathbb{P}(H^0(C, \Omega^1(\mathbb{Q}_p))) \to \mathbb{P}(H^0(\overline{C}, \Omega^1(\mathbb{F}_p)))$$

which preserves dimensions of subspaces. Let $\overline{\Lambda}$ be the linear subspace of $H^0(\overline{C}, \Omega^1(\mathbb{F}_p))$ corresponding to the image of $\mathbb{P}(\Lambda)$, which has dimension $\dim\Lambda$.

For any $\omega \in \mathbb{P}(H^0(C, \Omega^1(\mathbb{Q}_p)))$, we have $n(\omega, P) = v_P(\rho(\omega))$. Let D be the effective divisor on $\overline{C}$ defined as

$$D = \sum_{P\in\overline{C}} n(\Lambda, P)\cdot P$$

then $N(\Lambda, C/\mathbb{Q}_p) = \deg(D) \leq 2g-2$ and $\overline{\omega} \in \overline{\Lambda}$ implies $\operatorname{div}(\overline{\omega}) \geq D$. Therefore

$$N(\Lambda, C/\mathbb{Q}_p) \leq \max\{\deg(D) |\, D \geq 0, \dim\Omega(D) \geq \dim\Lambda\} = f_{C/\mathbb{F}_p}(\operatorname{codim}\Lambda)$$

□

Theorem 2.24. *Let $G, X, \overline{X}$ as above and $r = \operatorname{rank}(J(\mathbb{Q}))$. Then we have the bound*

$$\#X \leq \#\overline{X} + f_{C/\mathbb{F}_p}(r) + \Delta_p(\#\overline{X}, f_{C/\mathbb{F}_p}(r))$$

Furthermore, when $p > f_{C/\mathbb{F}_p}(r) + 2$, we have

$$\#X \leq \#\overline{X} + f_{C/\mathbb{F}_p}(r)$$

Proof. We have that

$$X = \bigcup_{P\in\overline{X}} (D_P \cap X) \Longrightarrow \#X = \sum_{P\in\overline{X}} \#(D_P \cap X)$$

Since the set D_P are pairwise disjoint. For each $P \in \overline{C}(\mathbb{F}_p)$ let $\omega_P \in A$ be "the best differential", i.e. such that $n(\omega_P, P) = n(A, P)$. So we have, by Proposition 2.22

$$\begin{aligned}
\#X = \sum_{P\in\overline{X}} \nu(P) &\leq \sum_{P\in\overline{X}} [1 + n(\omega_P, P) + \delta_p(n(\omega_P, P))] \\
&= \#\overline{X} + \sum_{P\in\overline{X}} [n(\omega_P, P) + \delta_p(n(\omega_P, P))] \\
&\leq \#\overline{X} + \sum_{P\in\overline{C}(\mathbb{F}_p)} n(\omega_P, P) + \sum_{P\in\overline{X}} \delta_p(n(\omega_P, P)) \\
&\leq \#\overline{X} + \sum_{P\in\overline{C}(\mathbb{F}_p)} n(A, P) + \sum_{P\in\overline{X}} \delta_p(n(A, P)) \\
&= \#\overline{X} + N(A, C/\mathbb{Q}_p) + \Delta_p(\#\overline{X}, N(A, C/\mathbb{Q}_p))
\end{aligned}$$

By theorem 2.23, $N(A, C/\mathbb{Q}_p) \leq f_{C/\mathbb{F}_p}(\operatorname{codim} A) = f_{C/\mathbb{F}_p}(r) \leq 2r$, since $\dim A = g - r$. By recalling that Δ_p is increasing in both arguments, we have

$$\begin{aligned} \#X &\leq \#\overline{X} + N(A, C/\mathbb{Q}_p) + \Delta_p(\#\overline{X}, N(A, C/\mathbb{Q}_p)) \\ &\leq \#\overline{X} + f_{C/\mathbb{F}_p}(r) + \Delta_p(\#\overline{X}, f_{C/\mathbb{F}_p}(r)) \end{aligned}$$

If we further suppose that $p > f_{C/\mathbb{F}_p}(r)+2$ then lemma 2.21 implies that $\Delta_p(\#\overline{X}, f_{C/\mathbb{F}_p}(r)) = 0$ and therefore

$$\#X \leq \#\overline{X} + f_{C/\mathbb{F}_p}(r)$$

□

In order to get an improvement of theorem 2.17, we simply notice that X contains $\mathcal{C}(\mathbb{Q})$ and therefore we have the following corollary.

Corollary 2.25 (Stoll, 2006). *Let $\mathcal{C}/\mathbb{Q}$ a curve of genus $g \geq 2$ with good reduction at $p > 2$. If $r = \operatorname{rank}(J(\mathbb{Q})) < g$, then*

$$\begin{aligned} \#\mathcal{C}(\mathbb{Q}) &\leq \#\overline{\mathcal{C}}(\mathbb{F}_p) + f_{\overline{\mathcal{C}}/\mathbb{F}_p}(r) + \Delta_p(\#\overline{\mathcal{C}}(\mathbb{F}_p), f_C(r)) \\ &\leq \#\overline{\mathcal{C}}(\mathbb{F}_p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor \end{aligned}$$

In particular, if $p > f_{\overline{\mathcal{C}}/\mathbb{F}_p}(r) + 2$ (notice that this is always true if $p > 2r + 2$), then

$$\#\mathcal{C}(\mathbb{Q}) \leq \#\overline{\mathcal{C}}(\mathbb{F}_p) + f_{\overline{\mathcal{C}}/\mathbb{F}_p}(r) \leq \#\overline{\mathcal{C}}(\mathbb{F}_p) + 2r$$

2.3.2 Curves with sharp Coleman's bound

So far we proved that, under some conditions, we can bound the number of rational points on a curve. However, we did not prove that this bound is the best possible, i.e. the inequality is actually an equality.

In Chapter 5 we will see some examples of genus 2 curves such that the Coleman's bound is sharp. However, we can construct potentially sharp curves of higher genus, following the ideas in [42].

Let $g \geq 2$ and suppose that either $2g + 1$ or $2g + 3$ is a prime number.

If $2g + 1 = p$ is prime, then $x^{2g+1} \equiv x \pmod{p}$ for every $x \in \mathbb{F}_p$ and therefore, if $c \in \mathbb{Z}$ is a quadratic nonresidue modulo p, then the only $\mathbb{F}_p$-rational point on the hyperelliptic curve

$$\overline{C}/\mathbb{F}_p : y^2 = x^{2g+1} - x + c$$

is the point at infinity. This means that every rational point reduces to the point at infinity modulo p, and this can only happen if they are not integers and have denominator divisible by p. Let $a_1, \ldots, a_{g-1} \in \mathbb{Z}$ not divisible by p with distinct absolute value and $b \in \mathbb{Z}$ an arbitrary lift of the inverse of $(a_1 \cdot a_2 \cdot \ldots \cdot a_{g-1})^2$ modulo p, then the hyperelliptic curve

$$C : y^2 : x^{2g+1} + b(a_1^2 - p^2x)(a_2^2 - p^2x) \ldots (a_{g-1}^2 - p^2x)(c - x)$$

has at least $2g-1$ rational points, namely:

$$\left(\frac{a_1^2}{p^2}, \pm\frac{a_1^{2g+1}}{p^{2g+1}}\right), \ldots, \left(\frac{a_{g-1}^2}{p^2}, \pm\frac{a_{g-1}^{2g+1}}{p^{2g+1}}\right), \infty$$

Notice that the reduction of C modulo p is exactly $\overline{C}$, so in this case the Coleman bound yields

$$2g-1 \leq C(\mathbb{Q}) \leq \overline{C}(\mathbb{F}_p) + 2g - 2 = 2g-1$$

if the rank of $J(\mathbb{Q})$ is less than g, which implies that $\#C(\mathbb{Q}) = 2g-1$. Moreover, corollary 2.25 implies that in this case the rank must exactly be $r = g-1$.

Example 2.26. Let $g = 3$ and $a_1 = 1$, $a_2 = 6$, $c = -1$, then we can take $b = 1$ and therefore we have the genus 3 curve

$$C_3 : y^2 = x^7 - (49x-1)(49x-36)(x+1)$$

Assuming GRH for `Magma` computations, we have that $\mathrm{rank}(J_3(\mathbb{Q})) = 2$ and hence we have a sharp Coleman bound for this curve, whose rational points are

$$\left(\frac{1}{49}, \pm\frac{1}{7^7}\right), \left(\frac{36}{49}, \pm\frac{6^7}{7^7}\right), \infty$$

If $2g+3 = p \geq 5$ is prime, then we claim that there exists a pair of consecutive quadratic nonresidues. If $p \equiv 1 \pmod 4$, then between 2 and $p-2$ there are exactly $\frac{p-1}{2}$ quadratic nonresidues and therefore two of them must be consecutive. On the other hand, if $p \equiv 3 \pmod 4$, then -1 and -4 are both quadratic nonresidues and thus, if either -2 or -3 is a nonresidue then we are done. If not, then 2 and 3 are both quadratic nonresidues. Now, let c and $c+1$ be two consecutive quadratic nonresidues modulo p and consider the hyperelliptic curve

$$\overline{C}/\mathbb{F}_p : y^2 = x^{2g+2} + c$$

which has only two $\mathbb{F}_p$-rational points, which are the points at infinity, since $x^{2g+2} = x^{p-1} \equiv 0, 1 \pmod p$, for every $x \in \mathbb{F}_p$, and therefore

$$y^2 = x^{2g+2} + c \equiv c, c+1 \pmod p$$

Now we want to find hyperelliptic curves whose reduction modulo p is $\overline{C}$.
Let $a_1, \ldots, a_{g-1} \in \mathbb{Z}$ not divisible by p and $b \in \mathbb{Z}$ an arbitrary lift of the inverse of $a_1 \cdot a_2 \cdot \ldots \cdot a_{g-1}$ modulo p, then the hyperelliptic curve

$$C : y^2 : x^{2g+2} + b(a_1 - px)(a_2 - px)\ldots(a_{g-1} - px)c$$

has at least $2g$ rational points, namely:

$$\left(\frac{a_1}{p}, \pm\frac{a_1^{g+1}}{p^{g+1}}\right), \ldots, \left(\frac{a_{g-1}}{p}, \pm\frac{a_{g-1}^{g+1}}{p^{g+1}}\right), \infty_{\pm}$$

As before, the reduction of C modulo p is exactly $\overline{C}$ and, if the rank of $J(\mathbb{Q})$ is less than g, we can compute the Coleman bound

$$2g \leq C(\mathbb{Q}) \leq \overline{C}(\mathbb{F}_p) + 2g - 2 = 2 + 2g - 2$$

which implies that $\#C(\mathbb{Q}) = 2g$. Again, by corollary 2.25, the rank must exactly be $r = g - 1$.

Example 2.27. Let $g = 4$, then $p = 2g + 3 = 11$, and we can choose $a_1 = 3$, $a_2 = 4$, $a_3 = 6$. Then we can take $b = 2$ and $c = 6$ (as 6 and 7 are both quadratic nonresidues modulo 11), so that we have the genus 4 curve

$$C_4 : y^2 = x^{10} - (11x - 3)(11x - 4)(11x - 6)$$

As in the example above, we can compute that $\mathrm{rank}(J_4(\mathbb{Q})) = 3$ and this means that the Coleman bound is again sharp. The eight rational points on C_4 are

$$\left(\frac{3}{11}, \pm\frac{3^5}{11^5}\right), \left(\frac{4}{11}, \pm\frac{4^5}{11^5}\right), \left(\frac{6}{11}, \pm\frac{6^5}{11^5}\right), \infty_{\pm}$$

Example 2.28. Let $g = 5$. Following the previous example, we can construct the genus 5 curve

$$C_5 : y^2 = x^{12} - (13x - 1)(13x - 2)(13x - 3)(13x - 12)$$

Again, we have $\mathrm{rank}(J_5(\mathbb{Q})) = 4$ and this means that the Coleman bound is sharp. The ten rational points on C_5 are

$$\left(\frac{1}{13}, \pm\frac{1^6}{13^6}\right), \left(\frac{2}{13}, \pm\frac{2^6}{13^6}\right), \left(\frac{3}{13}, \pm\frac{3^6}{13^6}\right), \left(\frac{12}{13}, \pm\frac{12^6}{13^6}\right), \infty_{\pm}$$

Chapter 3

Computational methods

In the previous chapter we described how to bound the number of rational points on a curve which satisfies some conditions. Now we want to explicitly compute those rational points.

In order to compute rational points via the *Chabauty-Coleman method*, we need to compute the finite set of p-adic points

$$\mathcal{C}(\mathbb{Q}_p)_1 := \left\{ z \in \mathcal{C}(\mathbb{Q}_p) : \int_{P_0}^{z} \omega = 0, \text{ for every } \omega \in A \right\}$$

where A is the subspace of annihilating differentials. By definition of A, this set contains $\mathcal{C}(\mathbb{Q})$, however we could have that $\mathcal{C}(\mathbb{Q}_p)_1$ strictly contains $\mathcal{C}(\mathbb{Q})$ or, even worse, it could be larger than the set of known rational points, so we need a way to provably extract $\mathcal{C}(\mathbb{Q})$. One solution for this problem is the *Mordell-Weil sieve*. (see appendix A)

We show the kind of problems that one could encounter in practice with the following example from [8, Ex. 1.22].

Example 3.1. We want to compute the rational points on the genus 2 curve

$$\mathcal{C} : y^2 = x^5 - 2x^3 + x + \frac{1}{4}$$

which has LMFDB label 971.a.971.1 (`https://www.lmfdb.org/Genus2Curve/Q/971/a/971/1`). It's easy to show that it has at least 7 rational points, namely

$$\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)$$

and we suspect that there aren't other rational points, but we need to prove that. Moreover, it can be shown that $J(\mathbb{Q}) \cong \mathbb{Z}$ and we will see that $[(-1, -1/2) - (0, 1/2)] \in J(\mathbb{Q})$ has infinite order. The conductor of $\mathcal{C}$ (i.e. the conductor of J) is $N = 971$, which is prime. So $\mathcal{C}$ has good reduction at every prime $p \neq 971$, in particular at $p = 3$, for which $\#\mathcal{C}(\mathbb{F}_3) = 7$ and therefore we can use corollary 2.25 and say that

$$\#\mathcal{C}(\mathbb{Q}) \leq \#\mathcal{C}(\mathbb{F}_3) + 2 \cdot 1 + \left\lfloor \frac{2 \cdot 1}{3 - 2} \right\rfloor = 11$$

So the Coleman bound isn't enough to prove that we have found all the rational points, and therefore we need to come up with a different strategy. We will work over $\mathbb{Q}_3$ and we will find an annihilating differential (notice that since $r = 1$ and $g = 2$, it is easy to show that $\dim(A) = 1$).

As for every hyperelliptic curve, a basis for $H^0(\mathcal{C}_{\mathbb{Q}_3}, \Omega^1)$ is given by

$$\omega_0 = \frac{dx}{2y} \qquad \text{and} \qquad \omega_1 = \frac{xdx}{2y}$$

So the annihilating differential η is just a $\mathbb{Q}_3$-linear combination of ω_0 and ω_1. We choose $P_0 = (0, 1/2)$ as the basepoint for the Abel-Jacobi map, so that we need η to satisfy

$$0 = \int_{(0,1/2)}^{(-1,-1/2)} \eta = \int_{(0,1/2)}^{(-1,-1/2)} (\alpha\omega_0 + \beta\omega_1) = \alpha \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 + \beta \int_{(0,1/2)}^{(-1,-1/2)} \omega_1$$

therefore we only need to compute $\int_{(0,1/2)}^{(-1,-1/2)} \omega_0$ and $\int_{(0,1/2)}^{(-1,-1/2)} \omega_1$, which we can do in `SageMath` with the following code:

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^3+x+1/4)
p = 3
K = Qp(p,15)
XK = X.change_ring(K)
XK.coleman_integrals_on_basis(XK(0,1/2),XK(-1,-1/2))
```

which outputs

```
3 + 3^2 + 3^4 + 3^5 + 2*3^6 + 2*3^7 + 2*3^8 + 3^10 + O(3^11),
2 + 2*3 + 2*3^3 + 3^4 + 3^6 + 2*3^8 + 2*3^9 + O(3^10),
2*3^-1 + 2*3 + 2*3^2 + 3^3 + 3^5 + 3^6 + 3^7 + O(3^9),
2*3^-2 + 3^-1 + 2 + 2*3 + 3^2 + 2*3^3 + 3^4 + 2*3^5 + 2*3^6 + 2*3^7 + O(3^8)
```

this means that

$$\int_{(0,1/2)}^{(-1,-1/2)} \omega_0 = 3 + 3^2 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{10} + O(3^{11})$$

$$\int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 2 + 2 \cdot 3 + 2 \cdot 3^3 + 3^4 + 3^6 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10})$$

(the last two lines of output correspond to the integrals of $\omega_2 = \frac{x^2dx}{2y}$ and $\omega_3 = \frac{x^3dx}{2y}$, which we don't need).

Clearly, if we choose $\alpha = \int_{(0,1/2)}^{(-1,-1/2)} \omega_1$ and $\beta = -\int_{(0,1/2)}^{(-1,-1/2)} \omega_0$, then

$$\alpha \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 + \beta \int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 0$$

which means that $\eta = \alpha\omega_0 + \beta\omega_1$ is an annihilating differential.

Now, we can use η to compute $\mathcal{C}(\mathbb{Q}_3)_1$, and in order to this we need to compute the Coleman integrals

$$\int_{(0,1/2)}^{P_t} \eta$$

where P_t ranges over all residue disks, and then find all the $z \in \mathcal{C}(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^{z} \eta = 0$.
In order to compute these integrals we can choose a lift Q of an $\mathbb{F}_3$-point in the same residue disk ad P_t and then write

$$\int_{(0,1/2)}^{P_t} \eta = \int_{(0,1/2)}^{Q} \eta + \int_{Q}^{P_t} \eta$$

The first integral is just a constant, while the second is a tiny integral which we can compute using a power series.

To sum up, the Coleman integrals that we need to compute are either tiny integrals, which are fairly easy to work with, or integrals between points which are not in the same residue disk, whose computation will be the subject of this chapter.

Remark 3.2. In the rest of the chapter we will explain how to compute Coleman integrals of regular 1-forms using the action of Frobenius on p-adic cohomology (following [8]), but there is an alternative approach.

In order to compute the Coleman integral $\int_P^Q \omega$, with $P, Q \in \mathcal{C}(\mathbb{Q}_p)$, we start by computing an integer k such that $k(P-Q) \in J(\mathbb{F}_p)$ is trivial (e.g. $k = \#J(\mathbb{F}_p)$). Then $D = [k(P-Q)] \in J(\mathbb{Q}_p)$ is in the same residue disk as 0, so we can compute

$$\int^{[P-Q]} \omega = \frac{1}{k} \int^{D} \omega$$

as a sum of tiny integrals.

This method has some limitations. First of all, there aren't implementations of Jacobian arithmetic over $\mathbb{Q}_p$ for all curves, but only for special classes, like the hyperelliptic curves. Secondly, this only applies to integrals of differentials of first kind, but there are other cases in which we want to compute integrals of differentials of second and third kind. Finally, we want to consider iterated integrals, which are not trivial to define on the Jacobian.

3.1 Construction of Coleman integrals in the rigid setting

We already saw how to construct an integration map in subsection 2.2.1, but that construction relied on the fact that the Jacobian is an abelian variety. Now we want to sketch a more general construction, but in order to do this, we need some deeper results, most of which we will not prove (for the missing proofs and other results from rigid geometry, see [18], [55] and [63]).

In this section K will be a p-adic field (i.e. a finitely generated extension of $\mathbb{Q}_p$) with ring of integers R, uniformizer π, and quotient field k.

Affine rigid geometry

Definition 3.3. The *Tate algebra* (or *Standard Affinoid algebra*) over K is defined, for each $n \in \mathbb{N}$, as

$$T_n := K\langle t_1, \dots, t_n \rangle := \left\{ \sum a_I t^I : \lim_{|I| \to \infty} |a_I| = 0 \right\}$$

Notice that this is a subring of the ring of formal power series $K\left[[t_1, \dots, t_n]\right]$.

In other words, the Tate algebra consists of the power series which converge on the unit polydisk $B_n := \left\{(z_1, \dots, z_n) \in \overline{K}^n : |z_i| \leq 1\right\}$.

Definition 3.4. A *Weierstrass polynomial* is a polynomial of the form

$$f(t_1, \dots, t_n) = t_1^m + t_1^{m-1} g_{m-1}(t_2, \dots, t_n) + \dots + g_0(t_2, \dots, t_n)$$

where $g_i \in T_{n-1}$ and $g_i(0, \dots, 0) = 0$ for every $i = 0, \dots, m-1$.

We have a slight modification of Weierstrass preparation theorem and division.

Theorem 3.5. *The following hold:*

1. *Let $f \in T_n$ such that $f(0, \dots, 0) = 0$. Suppose that the power series $f(t_1, \dots, t_n)$ has at least one term involving only one variable (which is always possible with a suitable change of variables), for instance t_1. Then we can write $f = uW$, where $u \in T_n^\times$ is a unit and W is a Weierstrass polynomial.*

2. *Given $f \in T_n$ and a Weierstrass polynomial g, there exists $q \in T_n$ and a Weierstrass polynomial r such that $f = gq + r$.*

From this one could prove that T_n is a Noetherian ring and a unique factorization domain.

We also have a version of Noether's normalization lemma, and therefore this ring satisfies the weak Nullstellensatz (i.e. every maximal ideal is a Galois conjugacy class of geometric points). More formally,

$$\text{mSpec}(T_n) = \left\{K\text{-homomorphisms } \psi : T_n \to \overline{K}\right\} / \text{Gal}(\overline{K}/K)$$

One can also show that $\text{mSpec}(T_n) \cong B_n / \text{Gal}(\overline{K}/K)$.

Definition 3.6. An *Affinoid algebra* is a K-algebra A with a surjective map $T_n \to A$, form some $n \in \mathbb{N}$.

Example 3.7. The prototypical example of affinoid algebra is $A = T_2/(t_1 t_2 - 1)$, which is a p-adic analogue of S^1. In this case we have:

$$\text{mSpec}(A) = \{(z_1, z_2) \in B_2 : z_1 z_2 = 1\} / \text{Gal}(\overline{K}/K) = \left\{x \in \overline{K} : |x| = 1\right\} / \text{Gal}(\overline{K}/K)$$

Remark 3.8. Define the *Gauss norm* of a series $f = \sum a_I t^I$, as $\|f\| = \max_I |a_I|$. Then T_n is a Banach algebra with respect to this norm. Since every ideal in the Tate algebra is topologically closed, the Gauss norm induces a norm on the quotients of T_n, and therefore every affinoid algebra inherits a structure of Banach algebra.

Monsky-Washnitzer cohomology

Definition 3.9. 1. The *standard weakly complete finitely generated algebra* (*wcfg* for short) is

$$\mathcal{T}_n^\dagger = \left\{ \sum a_I t^I : a_I \in R, \exists r > 1 \text{ s.t. } \lim_{|I|\to\infty} |a_I| r^{|I|} = 0 \right\}$$

2. A *wcfg algebra* is a R-algebra $A^\dagger$ with a surjective homomorphism $\mathcal{T}_n^\dagger \to A^\dagger$.

3. Given a wcfg algebra $A^\dagger$, its (π-adic) completion is given by $\widehat{A} := \varprojlim A^\dagger/\pi^n A^\dagger$.

Notice that the Gauss norm on the Tate algebra restricts to a norm on $\mathcal{T}_n^\dagger$ (although $\mathcal{T}_n^\dagger$ is not complete).

Differentials

The modules of differentials associated with $A^\dagger = \mathcal{T}_n^\dagger/\langle f_1, \ldots, f_m \rangle$ are

$$\Omega^1_{A^\dagger} := \frac{\bigoplus_{i=1}^n A^\dagger dt_i}{\left\langle \frac{\partial f_j}{\partial t_i} dt_i : j = 1, \ldots, m \right\rangle} \qquad \text{and} \qquad \Omega^k_{A^\dagger} := \bigwedge^k \Omega^1_{A^\dagger}$$

They are projective $A^\dagger$-modules and their associated de Rham complex $\Omega^\bullet_{A^\dagger}$ is

$$0 \to \Omega^0_{A^\dagger} \to \Omega^1_{A^\dagger} \to \ldots \to \Omega^k_{A^\dagger} \to \ldots$$

Cohomology

If $A^\dagger$ is a wcfg algebra, then $\overline{A} = A^\dagger/\pi$ is a finitely generated k-algebra.

Definition 3.10. The *Monsky-Washnitzer cohomology* of $\overline{A}$, denoted by $H_{MW}(\overline{A}/K)$, is the cohomology of the de Rham complex $\Omega^\bullet_{A^\dagger} \otimes K$.

In [11], Berthelot proved that $H^i_{MW}(\overline{A}/K)$ is a finite-dimensional K-vector space for every i.

Theorem 3.11. *1. Let $\overline{A}$ be a smooth finitely generated k-algebra. Then, there exists a flat wcfg algebra $A^\dagger$ such that $\overline{A} = A^\dagger/\pi$.*

2. *Any two such lifts are isomorphic.*

3. *Any morphism $\overline{f} : \overline{A} \to \overline{B}$ can be lifted to a morphism $f^\dagger : A^\dagger \to B^\dagger$.*

4. *Any two maps $f_1, f_2 : A^\dagger \to B^\dagger$ with the same reduction modulo π induce homotopic maps $\Omega^\bullet_{A^\dagger} \otimes K \to \Omega^\bullet_{B^\dagger} \otimes K$.*

Proof. See [18, Theorem 1.2.8.], [36] or [77]. □

From this result follows that the cohomology of $\overline{A}$ does not depend on the lift $A^\dagger$.

For computations we will need to compare the Monsky-Washnitzer cohomology with the de Rham cohomology, since the former works over fields of positive characteristic and is equipped with an action of Frobenius, and we want to have a similar action on the latter, which is defined over fields of characteristics 0. If we take $K = \mathbb{Q}_p$, then we have the following theorem.

Theorem 3.12 (Special case of Baldassarri-Chiarellotto [10] and Berthelot [11])**.** *Let Y be a smooth affine variety over $\mathbb{F}_p$ and $\widetilde{Y}$ a smooth affine variety over $\mathbb{Q}_p$ that is a lift of Y. Then the Monsky-Washnitzer cohomology of Y coincides with the algebraic de Rham cohomology of $\widetilde{Y}$:*

$$H^1_{\mathrm{dR}}(\widetilde{Y}) = H^1_{MW}(Y)$$

The lift of Frobenius

Theorem 3.11 implies that the map

$$\begin{aligned} \overline{A} &\to \overline{A} \\ x &\mapsto x^p \end{aligned}$$

(which is a well-defined ring homomorphism, since $\overline{A}$ is a ring of characteristic p) can be lifted to a map $A^\dagger \to A^\dagger$. However, we can say more:

Proposition 3.13. *Fix an automorphism σ of K that reduces to the p-power map on k and extend it to $\overline{K}$. Then there is a map $\phi : A^\dagger \to A^\dagger$ which is σ-linear and $\phi(x) \equiv x^p \pmod{\pi}$.*

The map ϕ in the statement of the previous Proposition induces, by functoriality, a σ-linear map

$$\phi : H^i_{MW}(\overline{A}/K) \to H^i_{MW}(\overline{A}/K)$$

Moreover, if $\#k = q = p^s$, the s-th iterate of $x \mapsto x^p$ is k-linear, so it lift induce a linear automorphism ϕ^s of $H^i_{MW}(\overline{A}/K)$.

In order to define Coleman integrals we need some information about the eigenvalues of this lift:

Theorem 3.14 (Chiarellotto [24])**.** *Each eigenvalue of ϕ^s acting on $H^i_{MW}(\overline{A}/K)$ is a q-Weil number*[1] *of integral weight contained in the interval $[i, 2i]$.*

Example 3.15 (Eigenvalues of Frobenius on the thrice-punctured projective line)**.** Consider $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ as a variety over $\mathbb{Q}_p$. As the ring of regular functions of an integral model w can take

$$A = \mathbb{Z}_p\left[x, y, z\right] / (xy - 1, (1 - x)z - 1)$$

[1] A *q-Weil number* of weight j is an algebraic number whose absolute value is $q^{j/2}$ under any complex embedding. Recall that $q = p^s = \#k$.

and we denote by $A^\dagger$ its weak completion, that is

$$A^\dagger = \left\{ \sum_{(i,j,k)\in\mathbb{N}^3} a_{i,j,k}x^i y^j z^k : a_{i,j,k} \in \mathbb{Z}_p,\ \exists r>1 \text{ s.t. } \lim_{i+j+k\to\infty} |a_{i,j,k}| r^{i+j+k} = 0 \right\} /(xy-1,(1-x)z-1)$$

A basis of $H^1_{MW}(\overline{A}/\mathbb{Q}_p)$ is given by $\omega_1 = \frac{dx}{x}$ and $\omega_2 = \frac{dx}{1-x}$ (or, more formally, by $\omega_1 = ydx$ and $\omega_2 = zdx$).

As a lift of Frobenius we can take

$$F : x \mapsto x^p, y \mapsto y^p$$

however, we need to be more careful when defining $F(z)$. As a matter of fact, we have

$$1 = F(1-x)F(z) = (1-x^p)F(z)$$

so we have

$$F(z) = \frac{1}{1-x^p} = \frac{1}{(1-x)^p + (1-x^p) - (1-x)^p}$$

We want to show that $F(z)$ can be written as an element of $A^\dagger$. In order to do this, let $H_p(x) = \frac{(1-x)^p - (1-x^p)}{p} \in \mathbb{Z}_p[x]$, so that

$$\begin{aligned} F(z) &= \frac{1}{(1-x)^p + (1-x^p) - (1-x)^p} = \frac{1}{(1-x)^p - pH_p(x)} \\ &= \frac{z^p}{(z(1-x))^p - pz^pH_p(x)} = \frac{z^p}{1-pz^pH_p(x)} = z^p \sum_{n\geq 0} (pz^pH_p(x))^n \end{aligned}$$

so we only need to show that the series $z^p \sum (pz^pH_p(x))^n$ converges on a polydisk of radius strictly greater than 1. Since y does not appear in the series, we will only work with x and z. We claim that the series converges on

$$B := \left\{ (x,z) \in \mathbb{Q}_p^2 : v_p(x) \geq -\frac{1}{4p}, v_p(z) \geq -\frac{1}{4p} \right\} = \left\{ (x,z) \in \mathbb{Q}_p^2 : |x|_p \leq p^{\frac{1}{4p}}, |z|_p \leq p^{\frac{1}{4p}} \right\}$$

(notice that $p^{\frac{1}{4p}} > 1$ for every p). Indeed, if $(x,z) \in B$, then

$$\begin{aligned} v_p(pz^pH_p(x)) &= 1 + pv_p(z) + v_p(H_p(x)) \geq 1 + pv_p(z) + \min\{\deg(H_p(x))v_p(x), 0\} \\ &\geq 1 + \left(-\frac{1}{4}\right) - p\cdot\frac{1}{4p} = \frac{1}{2} \end{aligned}$$

thus $|(pz^pH_p(x))^n|_p \leq p^{-\frac{n}{2}} \to 0$, if $n \to \infty$. So the series converges on B, proving that $F(z) \in A^\dagger$. Moreover, it is clear that $F(z) \equiv z^p \pmod p$, so F is a lift of Frobenius.

We can now compute the action of this lift on the Monsky-Washnitzer cohomology. We just have to compute this action (given by the pull-back of F) on the elements of a basis:

$$F^*\omega_1 = F^*(ydx) = y^p \cdot px^{p-1}dx = pydx = p\omega_1$$

$$F^*\omega_2 = F^*(zdx) = z^p \sum_{n\geq 0} (pz^pH_p(x))^n \cdot px^{p-1}dx$$

In order to simplify the last expression we need to compute the cohomology class of $F^*\omega_2$. We start by writing $F^*\omega_2 = a\omega_1 + b\omega_2 + \psi$, where a, b are constants and ψ is an exact form. Then a, b can be computed by looking at the residues of $F^*\omega_2$ at $x = 0$ and $x = 1$. For instance, we can notice that $F^*\omega_2$ is regular at $x = 0$, so that $a = 0$ because ω_1 is not regular at $x = 0$.

In order to compute b, we divide the cases $p = 2$ and p odd. We start with the odd case first: recall that by definition $\deg(H_p(x)) = p - 1$ and $z = (1 - x)^{-1}$, so that when we write $pz^pH_p(x)$ as a Laurent series in $(x - 1)$, the term with highest degree in the series has degree $-p + (p - 1) = -1$. Furthermore,

$$\begin{aligned} pz^px^{p-1}dx &= p(1-x)^{-p}x^{p-1}dx = p(1-x)^{-p}(1+(x-1))^{p-1}dx \\ &= p(1-x)^{-p}\sum_{j=0}^{p-1}\binom{p-1}{j}(x-1)^j dx \\ &= -p\sum_{j=0}^{p-1}\binom{p-1}{j}(x-1)^{j-p}dx \end{aligned}$$

contains only terms of negative degree in $(x - 1)$. Now we can write

$$F^*\omega_2 = pz^px^{p-1}\sum_{n\geq 0}\left(pz^pH_p(x)\right)^n dx = pz^px^{p-1}dx + pz^px^{p-1}\sum_{n\geq 1}\left(pz^pH_p(x)\right)^n dx$$

however, when we write the second term as a Laurent series in $(x - 1)$ we only get terms of degree ≤ -2, which means that it has residue 0 (and therefore is an exact form). So the residue of $F^*\omega_2$ comes only from the term $pz^px^{p-1}dx$ which, using the computations above, can be written as

$$\begin{aligned} pz^px^{p-1}dx &= -p\sum_{j=0}^{p-1}\binom{p-1}{j}(x-1)^{j-p}dx \\ &= -p(x-1)^{-1}dx + (\text{terms of degree } \leq -2)dx \\ &= p\omega_2 + \text{exact form} \end{aligned}$$

which means that $F^*\omega_2 = p\omega_2 + \psi$.

Similarly, if $p = 2$, then we can compute $F^*\omega_2$ and get

$$\begin{aligned} F^*\omega_2 &= 2z^2x\sum_{n\geq 0}2^n\left(z^2H_2(x)\right)^n dx \\ &= 2z^2x\sum_{n\geq 0}2^n\left((1-x)^{-2}(x^2-x)\right)^n dx \\ &= 2\left(\frac{1}{(1-x)^2} - \frac{1}{1-x}\right)\sum_{n\geq 0}2^n\left(1-\frac{1}{1-x}\right)^n dx \\ &= \text{exact form} - \frac{2dx}{1-x}\sum_{n\geq 0}2^n \\ &= \frac{2dx}{1-x} + \text{exact form} = 2\omega_2 + \text{exact form} \end{aligned}$$

since in the 2-adic topology we have $\sum_{n\geq 0} 2^n = -1$.

Therefore the action of Frobenius on $H^1_{MW}(\overline{A}/\mathbb{Q}_p)$ is just the multiplication by p.

Specialization and the algebra of locally analytic functions

Let $A^\dagger = \mathcal{T}_n^\dagger/I$ be a wcfg algebra. The completion of $A^\dagger$ with respect to the Gauss norm induced from $\mathcal{T}_n^\dagger$ is the algebra $A = T_n/I$. We then obtain an affinoid space $X = \text{mSpec}(A)$ and a reduction $X_k = \text{Spec}(\overline{A})$. The geometric points X^{geo} of X are the K-linear homomorphisms $A \to \overline{K}$.

There is a reduction map, defined on the geometric points:

$$X^{geo} \to X_k$$
$$(\psi : A \to L \subset \overline{K}) \mapsto (\overline{\psi} : A/\pi \to \mathcal{O}_L/\pi_L)$$

Definition 3.16. A *residue disk* U_x is the inverse image in X^{geo} of a geometric point $x : \text{Spec}(\overline{k}) \to X_k$ under the reduction map. By smoothness and Hensel's lemma, one can show that U_x is isomorphic to the space of geometric points of a unit polydisk.

Definition 3.17. A *K-locally analytic function* on X is a map

$$f : X^{geo} \to \overline{K}$$

such that

- f is $\text{Gal}(\overline{K}/K)$-equivariant, i.e. for any $\tau \in \text{Gal}(\overline{K}/K)$ we have $f(\tau(x) = \tau(f(x))$
- On each residue disk, f is defined by a convergent power series.

The K-locally analytic functions on X form a K-algebra A_{loc} containing A.

Now we want to define how ϕ acts on points and functions.
Given a morphism $\psi : A \to L \subset \overline{K})$ (which is a geometric point of X) we define

$$\phi(\psi) = \sigma^{-1} \circ \psi \circ \phi$$

and if f is a K-locally analytic function we define

$$\phi(f)(x) = \sigma(f(\phi(x)))$$

where σ is an automorphism of K as in Proposition 3.13.

Construction of the Coleman integral

Now we can construct the Coleman integral on an affinoid space, following [12].

Theorem 3.18. *Let $A^\dagger$ be a wcfg algebra. Then there is a unique K-linear integration map*

$$\int : \left(\Omega^1_{A^\dagger} \otimes K\right)^{d=0} \to A_{loc}/K$$

satisfying:

1. *$d \circ \int$ is the canonical map $\left(\Omega^1_{A^\dagger} \otimes K\right)^{d=0} \to \Omega^1_{A_{loc}}$*
2. *$\int \circ d$ is the canonical map $A^\dagger \otimes K \to A_{loc}/K$*
3. *$\phi \circ \int = \int \circ \phi$*

Proof. Choose forms $\omega_1, \dots, \omega_r \in \Omega_{A^\dagger} \otimes K$ whose images in $H^1_{MW}(\overline{A}/K)$ form a basis. Notice that now we only need to integrate the ω_i's, since a general 1-form ω has the form $\omega = df + \sum \alpha_i \omega_i$, for some $A^\dagger \otimes K$-function f, and therefore the formal properties of integration imply that $\int \omega = f + \sum \alpha_i \int \omega_i$.

Let $\underline{\omega}$ be the (column) vector of the forms ω_i, then there is a matrix $M \in K^{r \times r}$ such that

$$\phi\underline{\omega} = M\underline{\omega} + d\underline{g}$$

for some $g \in (A^\dagger \otimes K)^r$. Applying $\int$ to this identity and using linearity and the third property we get

$$\phi \int \underline{\omega} = M \int \underline{\omega} + \underline{g}$$

Fix a vector of functions $F_{\underline{\omega}}$ representing $\int \underline{\omega}$, so that we can rewrite the previous equality as

$$\phi F_{\underline{\omega}} = M F_{\underline{\omega}} + g + \underline{c}$$

for some vector of constants $\underline{c}$. Then we will need the following lemma (see below for the proof)

Lemma 3.19. *The map $\sigma - M : K^r \to K^r$ is bijective.*

This lemma implies that there exists a vector of constants $\underline{d}$ such that $(\sigma - M)(\underline{d}) = -\underline{c}$. Since integration is defined up to constants, we can replace $F_{\underline{\omega}}$ with $F_{\underline{\omega}} + \underline{d}$, so that we can always choose $\underline{c} = 0$, since

$$\phi(F_{\underline{\omega}} + \underline{d}) - M(F_{\underline{\omega}} + \underline{d}) = \underline{g} + \underline{c} + (\sigma - M)(\underline{d}) = \underline{g} + \underline{c} - \underline{c} = \underline{g}$$

since $\phi \equiv \sigma$ on K. Because $dF_{\underline{\omega}} = \underline{\omega}$, we only need to compute $F_{\underline{\omega}}$ on a single point in each residue disk. This is true since on a residue disk the formal integral makes sense by definition of $\Omega^1_{A^\dagger}$, so that $F_{\underline{\omega}}$ and the formal integral of $\underline{\omega}$ differ at most by a constant.
Take an arbitrary point x, then:

$$\sigma F_{\underline{\omega}}(\phi x) = (\phi F_{\underline{\omega}})(x) = M F_{\underline{\omega}}(x) + \underline{g}(x)$$

Since x and ϕx are in the same residue disk, the difference $F_{\underline{\omega}}(\phi x) - F_{\underline{\omega}}(x) = \underline{e}(x)$ is uniquely determined by $\underline{\omega}$ (and it can be found with formal integration). So we can rewrite the last equation as

$$(\sigma - M)(F_{\underline{\omega}}(x)) = \underline{g}(x) - \sigma(\underline{e}(x))$$

Therefore, since $\sigma - M$ is bijective, we uniquely determine $F_{\underline{\omega}}(x)$. The properties in the statement are now trivial by construction. □

Proof of Lemma 3.19. Since the map is linear and the spaces are finite dimensional, we only need to show that $\sigma - M$ is injective.

Fix $c \in K^r$ and consider the equation $(\sigma - M)x = c$, or equivalently, $\sigma x = Mx + c$. Applying σ to both sides yields

$$\sigma^2 x = \sigma(Mx) + \sigma(c) = \sigma(M)\sigma(x) + \sigma(c) = \sigma(M)(Mx + c) + \sigma(c)$$

Then if $\#k = p^s$, then $\sigma^s \equiv \mathrm{id}_{K^r}$, so that

$$x = \sigma^s(x) = \sigma(M)^{s-1} \cdot \sigma(M)^{s-2} \cdot \ldots \cdot \sigma(M) \cdot Mx + \widetilde{c}$$

where $\widetilde{c}$ is an element of K^r which can be written (albeit in a very convoluted way) in terms of σ, M and c. Now notice that $\widetilde{M} = \sigma(M)^{s-1} \cdot \sigma(M)^{s-2} \cdot \ldots \cdot \sigma(M) \cdot M$ is precisely the matrix of the "linear Frobenius" ϕ^s when it acts on $H^1_{MW}(\overline{A}/K)$. Theorem 3.14 implies that 1 is not an eigenvalue of $\widetilde{M}$, so the matrix $I - \widetilde{M}$ is invertible.

Finally, we rewrite the equation $x = \widetilde{M}x + \widetilde{c}$ as $(I - \widetilde{M})x = \widetilde{c}$, which proves that it has only one solution and therefore the original equation $(\sigma - M)x = c$ must have at most one solution as well. □

3.2 Algorithms for Coleman integrals

Let's start with some definitions.

Definition 3.20. Let $\mathcal{C}/\mathbb{Q}$ be a curve. We define the associated rigid analytic space $\mathcal{C}^{an}$ as follows. Let $\mathcal{X}$ be a smooth curve over $\mathbb{Z}_p$ such that

$$\mathcal{X} \otimes \mathbb{Q}_p \cong \mathcal{C} \otimes \mathbb{Q}_p$$

then $\mathcal{C}^{an}$ is the generic fiber of $\mathcal{X}$. (for more information about the analytification functor see [15])

Definition 3.21. A wide open subspace of $\mathcal{C}^{an}$ is the complement in $\mathcal{C}^{an}$ of the union of finitely many disjoint closed disks of radius < 1.

The following theorem shows more properties of the Coleman integral

Theorem 3.22 (Coleman [28], Coleman-de Shalit[29])**.** *Let η, ξ be 1-forms on a wide open subspace V of $\mathcal{C}^{an}$, $P, Q, R \in V(\overline{\mathbb{Q}_p})$ and $a, b \in \overline{\mathbb{Q}_p}$. The definite Coleman integral has the following properties:*

1. *(Linearity)*
$$\int_P^Q a\eta + b\xi = a\int_P^Q \eta + b\int_P^Q \xi$$
2. *(Additivity in endpoints)*
$$\int_P^Q \eta = \int_P^R \eta + \int_R^Q \eta$$

3. *(Change of variables) If $V' \subseteq X$ is a wide open subspace of a rigid analytic space X, ω a 1-form on V' and $\phi : V \to V'$ a rigid analytic map, then*

$$\int_P^Q \phi^*\omega = \int_{\phi(P)}^{\phi(Q)} \omega$$

4. *(Fundamental theorem of Calculus) For every rigid analytic function f on V*

$$\int_P^Q df = f(Q) - f(P)$$

5. *(Galois compatibility) If $P, Q \in V(\mathbb{Q}_p)$ and η is defined over $\mathbb{Q}_p$, then $\int_P^Q \eta \in \mathbb{Q}_p$.*

Our goal is to integrate differential 1-forms of the first kind, but we will do more and show how to integrate differentials of the second kind.

We will first explain the algorithms for hyperelliptic curves and then we will move on to the general case.

For simplicity, we will assume that $\mathcal{C}$ is a genus g hyperelliptic curve over $\mathbb{Q}$ with equation $y^2 = P(x)$, where P is a monic polynomial of degree $2g+1$ with no repeated roots. Suppose that $p \neq 2$ is a prime of good reduction for $\mathcal{C}$, consider $\overline{\mathcal{C}}/\mathbb{F}_p$, with affine equation $y^2 = \overline{P}(x)$ and take $C = \overline{\mathcal{C}} \setminus \{\infty, y = 0\}$.

Let $A = \mathbb{Z}_p\left[x, y, y^{-1}\right]/(y^2 - P(x))$ be the coordinate ring of $\mathcal{C}$ and let $A^\dagger$ be the weak completion of A. As in example 3.15 we have:

$$A^\dagger = \left\{ \sum_{(i,j,k)\in\mathbb{N}^3} a_{i,j,k} x^i y^j (y^{-1})^k : a_{i,j,k} \in \mathbb{Z}_p,\ \exists r > 1 \text{ s.t. } \lim_{i+j+k\to\infty} |a_{i,j,k}| r^{i+j+k} = 0 \right\} / (y^2 - P(x))$$

Alternatively, the elements of $A^\dagger$ can be written as series of the form

$$\sum_{n=-\infty}^{\infty} (S_n(x) + T_n(x)y)y^{2n}$$

where S_n, T_n are polynomials of degree at most $2g$ such that

$$\liminf_{n\to\infty} \frac{v_p(S_n)}{n} \qquad \liminf_{n\to\infty} \frac{v_p(S_{-n})}{n} \qquad \liminf_{n\to\infty} \frac{v_p(T_n)}{n} \qquad \liminf_{n\to\infty} \frac{v_p(T_{-n})}{n}$$

are all positive. Here $v_p\left(\sum_{i=0}^d a_i x^i\right) = \max\{v_p(a_i) : 0 \leq i \leq d\}$.

Recall that, by Theorem 3.12, the Monsky-Washnitzer cohomology of C coincides with the de Rham cohomology of $\mathcal{C}$ (i.e. $H^1_{\mathrm{dR}}(A)$). Then we have the following result.

Proposition 3.23. *The first de Rham cohomology of A splits into two eigenspaces under the hyperelliptic involution*

$$C \to C, \quad (x, y) \mapsto (x, -y)$$

The first eigenspace $H^1(A)^+$ is the positive eigenspace generated by

$$\left\{ \frac{x^i dx}{y^2} : i = 0, \ldots, 2g \right\}$$

and the second eigenspace $H^1(A)^-$ is the negative eigenspace generated by

$$\left\{ \frac{x^i dx}{y} : i = 0, \dots, 2g-1 \right\}$$

We saw earlier that passing to $A^\dagger$ does not change the cohomology, but we have the advantage of explicit computations for the action of Frobenius on $H^1(A^\dagger)^-$. To do this we need to lift the p-power Frobenius to an endomorphism σ of $A^\dagger$.

On $\mathbb{Z}_p[x]$, we define σ by $x^\sigma = x^p$ and then extend it additively. To define y^σ, we recall that $y^2 = P(x)$ both in A and $A^\dagger$, so we must have the following identity:

$$(y^\sigma)^2 = (y^2)^\sigma = (P(x))^\sigma = P(x)^\sigma \left(\frac{y^2}{P(x)} \right)^p = \frac{y^{2p} P(x)^\sigma}{P(x)^p}$$

and therefore we have

$$\sigma : y \mapsto y^p \left(\frac{P(x)^\sigma}{P(x)^p} \right)^{\frac{1}{2}}$$

To prove p-adic convergence we slightly rewrite y^σ as

$$y^\sigma = y^p \left(1 + \frac{P(x)^\sigma - P(x)^p}{P(x)^p} \right)^{\frac{1}{2}}$$

and then use the Taylor expansion for $(1+t)^{-\frac{1}{2}}$ to get

$$\frac{1}{y^\sigma} = \frac{1}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{P(x)^\sigma - P(x)^p}{P(x)^p} \right)^j = \frac{1}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{P(x)^\sigma - P(x)^p}{y^{2p}} \right)^j \tag{3.1}$$

Now, we note that $P(x)^\sigma - P(x)^p$ is divisible by p, so the summands go to 0 when $j \to \infty$, proving p-adic convergence.

Remark 3.24. Now we see why we removed $y = 0$ from $\overline{\mathcal{C}}$, since in those points the series may diverge. It is possible to compute a Frobenius lift without deleting $y = 0$ but it would be more difficult.

Finally, we extend the action of the p-power Frobenius to differentials by writing

$$\sigma^* : dx \mapsto d(x^p) = p x^{p-1} dx$$

To prove Proposition 3.23 and to compute expressions of the form $\left(\frac{x^i dx}{y} \right)^\sigma$, we need two reduction lemmas.

Lemma 3.25 (Kedlaya [47])**.** *Let $R(x), Q_1(x), Q_2(x) \in \mathbb{Q}_p[x]$ such that*

$$R(x) = P(x) Q_1(x) + P'(x) Q_2(x)$$

then

$$\frac{R(x)dx}{y^s} = \left(Q_1(x) + \frac{2Q_2'(x)}{s-2} \right) \frac{dx}{y^{s-2}}$$

as elements of $H^1_{MW}(C)$.

Proof. We have

$$\begin{aligned}\frac{R(x)dx}{y^s} &= \frac{P(x)Q_1(x)dx}{y^s} + \frac{P'(x)Q_2(x)dx}{y^s} \\ &= \frac{y^2Q_1(x)dx}{y^s} + \frac{P'(x)Q_2(x)dx}{y^s} = \frac{Q_1(x)dx}{y^{s-2}} + \frac{P'(x)Q_2(x)dx}{y^s}\end{aligned}$$

since $y^2 = P(x)$. For the second term we have

$$\frac{Q_2(x)P'(x)dx}{y^s} = \frac{2Q_2(x)dy}{y^{s-1}}$$

since $P'(x)dx = d(P(x)) = d(y^2) = 2ydy$. Then

$$\frac{2Q_2(x)dy}{y^{s-1}} = -\frac{2Q_2(x)d(y^{-(s-2)})}{s-2}$$

as $d\left(\frac{1}{y^{s-2}}\right) = -\frac{(s-2)dy}{y^{s-1}}$. Finally,

$$-\frac{2Q_2(x)d(y^{-(s-2)})}{s-2} = \frac{2Q_2'(x)dx}{(s-2)y^{s-2}}$$

because in $H^1_{MW}(C)$

$$0 \equiv d\left(\frac{Q_2(x)}{y^{s-2}}\right) = \frac{d(Q_2(x))}{y^{s-2}} + Q_2(x)d\left(\frac{1}{y^{s-2}}\right) = \frac{Q_2'(x)dx}{y^{s-2}} + Q_2(x)d\left(\frac{1}{y^{s-2}}\right)$$

which implies $\frac{Q_2'(x)dx}{y^{s-2}} = -Q_2(x)d(y^{-(s-2)})$. Putting everything together yields

$$\frac{Q_2(x)P'(x)dx}{y^s} = \frac{2Q_2'(x)dx}{(s-2)y^{s-2}}$$

and this concludes the proof. □

Moreover, since $dy = \frac{P'(x)dx}{2y}$, we can also compute

$$\begin{aligned}d(x^iy^j) &= ix^{i-1}y^jdx + x^i \cdot jy^{j-1}dy \\ &= ix^{i-1}y^jdx + x^i \cdot jy^{j-1}\frac{P'(x)dx}{2y} = \frac{(2ix^{i-1}y^{j+1} + jx^iP'(x)y^{j-1})dx}{2y}\end{aligned}$$

Then, the monomial with largest degree in the formula above is $x^{i-1}y^{j+1}$ if $1 \leq i \leq 2g$ and $x^{2g}y^{j-1}$ if $i = 0$. Similarly, the monomial with the smallest degree is x^ky^{j-1} with $0 \leq k \leq 2g$. As a special case we get

$$\begin{aligned}d(2Q(x)y) &= 2Q(x)dy + 2Q'(x)ydx \\ &= 2Q(x)\frac{P'(x)dx}{2y} + 2Q'(x)ydx \\ &= \frac{(Q(x)P'(x) + 2Q'(x)P(x))dx}{y}\end{aligned}$$

which proves the second reduction lemma.

Lemma 3.26 (Kedlaya [47]). *For any polynomial $Q(x) \in \mathbb{Q}_p[x]$ we have*

$$\frac{(Q(x)P'(x) + 2Q'(x)P(x))dx}{y} = d(2Q(x)y) = 0$$

as elements of $H^1_{MW}(C)$.

Now we are ready to prove Proposition 3.23.

Proof of Proposition 3.23. We only need to show that every element of $H^1_{\mathrm{dR}}(A)$ can be written as

$$\frac{Q_1(x)dx}{y} + \frac{Q_2(x)dx}{y^2}$$

with $\deg(Q_1(x)) \leq 2g-1$ and $\deg(Q_2(x)) \leq 2g$. Indeed, any element of $H^1_{\mathrm{dR}}(A)$ can be written as

$$\sum_{n=-\infty}^{\infty} \frac{Q_n(x)dx}{y^n}$$

where $Q_n(x) \in \mathbb{Q}_p[x]$ are almost all zero. To simplify this expression notice that for every $Q(x) \in \mathbb{Q}_p[x]$ we have

$$0 = d\left(\frac{Q(x)}{y^n}\right) = \frac{d(Q(x))}{y^n} + Q(x)d\left(\frac{1}{y^n}\right)$$

as elements of $H^1_{\mathrm{dR}}(A) = H^1_{MW}(C)$. It follows that

$$\frac{Q'(x)dx}{y^n} = \frac{nQ(x)dy}{y^{n+1}} = \frac{nQ(x)P'(x)dx}{2y^{n+2}}$$

and therefore we can reduce all the terms $\frac{Q_n(x)dx}{y^n}$ with $n < 0$ to the cases $n = 1$ and $n = 0$ (which is trivial, see below). On the other hand, when $n > 2$ we can use repeatedly Lemma 3.25 (because $\gcd(P(x), P'(x)) = 1$, as P has no repeated roots) to reduce n to 1 or 2. This proves that every element of $H^1_{\mathrm{dR}}(A)$ can be represented as

$$\frac{\widetilde{Q_1}(x)dx}{y} + \frac{\widetilde{Q_2}(x)dx}{y^2}$$

where $\widetilde{Q_1}(x), \widetilde{Q_2}(x) \in \mathbb{Q}_p[x]$. If $\deg(\widetilde{Q_2}(x)) > 2g$, then there exist $S(x), R(x) \in \mathbb{Q}_p[x]$ such that

$$\widetilde{Q_2}(x) = S(x)P(x) + R(x) \qquad \text{and} \quad \deg(R(x)) \leq 2g$$

Thus

$$\frac{\widetilde{Q_2}(x)dx}{y^2} = \frac{(S(x)P(x) + R(x))dx}{y^2} = \frac{(S(x)y^2 + R(x))dx}{y^2} = S(x)dx + \frac{R(x)dx}{y^2}$$

Clearly, there exists $\widetilde{S}(x) \in \mathbb{Q}_p[x]$ such that $S(x) = \widetilde{S}'(x)$ and therefore $S(x)dx = d(\widetilde{S}(x)) = 0$ in $H^1_{\mathrm{dR}}(A)$. So

$$\frac{\widetilde{Q_2}(x)dx}{y^2} = S(x)dx + \frac{R(x)dx}{y^2} = \frac{R(x)dx}{y^2}$$

and $\deg(R(x)) \leq 2g$, as desired.

If $\deg(\widetilde{Q_1}(x)) = m \leq 2g$, then notice that Lemma 3.26 with $Q(x) = x^{m-2g}$ implies that

$$\frac{\left[x^{m-2g}P'(x) + 2(m-2g)x^{m-2g-1}P(x)\right]dx}{y} = 0$$

and note that the polynomial $x^{m-2g}P'(x) + 2(m-2g)x^{m-2g-1}P(x)$ has degree m and leading term $(2g+1) + 2(m-2g) = 2m - 2g + 1 \neq 0$, so a suitable multiple can be subtracted from $\widetilde{Q_1}(x)$ to reduce its degree at least by 1. Carrying out this process repeatedly reduces $\widetilde{Q_1}(x)$ to a polynomial of degree $\leq 2g-1$ and we are done. □

In order to compute $\left(\frac{x^i dx}{y}\right)^\sigma$ we use the definition of σ to expand the expression and then we reduce it with the two lemmas, like we did in the previous proof. Indeed, we have

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{1}{y^\sigma} p x^{pi+p-1} dx$$

we then use equation 3.1 to get the infinite series

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{p x^{pi+p-1}}{y^p} \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j} \left(\frac{P(x)^\sigma - P(x)^p}{y^{2p}}\right)^j dx$$

Remark 3.27. If we apply the hyperelliptic involution to $\left(\frac{x^i dx}{y}\right)^\sigma$ we see that it changes sign. In other words $\left(\frac{x^i dx}{y}\right)^\sigma \in H^1(A)^-$ and therefore can be written as a linear combination of the generators of $H^1(A)^-$ (see Proposition 3.23).

We want to implement this procedure on a computer, so we will have to take a truncation of this series, i.e. the computer will compute

$$\frac{p x^{pi+p-1}}{y^p} \sum_{j=0}^{L} \binom{-\frac{1}{2}}{j} \left(\frac{P(x)^\sigma - P(x)^p}{y^{2p}}\right)^j dx$$

So, the natural question now is: How large L must be to get provably correct calculations (i.e. to be sure of a certain number of digits of the results)? Suppose that we have computed such precision, so that

$$\frac{p x^{pi+p-1}}{y^p} \sum_{j=0}^{L} \binom{-\frac{1}{2}}{j} \left(\frac{P(x)^\sigma - P(x)^p}{y^{2p}}\right)^j dx = \sum_{j=-L_1}^{L_2} \frac{R_j(x)dx}{y^{2j+1}}$$

Now, we use the reduction lemmas to eliminate the $j = L_2$ term, then the $j = L_2 - 1$ term, and so on until there are no term with $j > 0$. We do the same thing to eliminate the terms with $j < 0$, so that at the end there is only the term with $j = 0$, i.e.

$$\left(\frac{x^i dx}{y}\right)^\sigma = dh_i + \sum_{j=0}^{2g-1} M_{ji} \frac{x^j dx}{y}$$

However, $dh_i \equiv 0$ in $H^1_{MW}(C)$, so we have that the action of σ on $H^1(A)^-$ is linear and it is given by the Frobenius matrix $\mathbf{M} = (M_{ji})_{i,j=0,\ldots,2g-1}$.

Precision is lost when we divide by p during the reduction algorithm, so we need to measure the loss of precision at each step to keep count of how many provably correct digits we have.

Lemma 3.28 ([47, Lemma 2]). *Let $A(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree $\leq 2g$ and consider the reduction of*

$$\omega = \frac{A(x)dx}{y^{2m+1}}$$

By Lemma 3.25 we can write

$$\omega = \frac{A(x)dx}{y^{2m+1}} = df + \frac{B(x)dx}{y}$$

where $B(x) \in \mathbb{Q}_p[x]$ has degree $\leq 2g-1$ and

$$f = \sum_{k=-1}^{m-1} \frac{F_k(x)}{y^{2k+1}}$$

with $\deg F_k \leq 2g$. Then

$$p^{\lfloor \log_p(2m-1) \rfloor} B(x) \in \mathbb{Z}_p[x]$$

Lemma 3.29 ([47, Lemma 3]). *Let $A(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree $\leq 2g$ and consider the reduction of*

$$\omega = A(x)y^{2m-1}dx = \frac{(A(x)y^{2m})dx}{y}$$

By Lemma 3.26 we can write

$$\omega = \frac{A(x)y^{2m})dx}{y} = df + \frac{B(x)dx}{y}$$

where $B(x) \in \mathbb{Q}_p[x]$ has degree $\leq 2g-1$ and

$$f = Cy^{2m+1} + \sum_{k=0}^{m-1} F_k(x)y^{2k+1}$$

with $\deg F_k \leq 2g$ and $C \in \mathbb{Q}_p$. Then

$$p^{\lfloor \log_p((2g+1)(2m+1)) \rfloor} B(x) \in \mathbb{Z}_p[x]$$

Combining Lemma 3.28 and 3.29 we can prove the following Proposition.

Proposition 3.30 ([23, page 34]). *To get N correct digits in the matrix of Frobenius $\mathbf{M}$, we need to start with precision*

$$N_1 = N + \max\{\lfloor \log_p(2N_2 - 3) \rfloor, \lfloor \log_p(2g+1) \rfloor\} + 1 + \lfloor \log_p(2g-1) \rfloor$$

where N_2 is the smallest integer such that

$$N_2 - \max\{\lfloor \log_p(2N_2+1) \rfloor, \lfloor \log_p(2g+1) \rfloor\} \geq N$$

In particular, we can just need to compute

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{px^{pi+p-1}}{y^p} \sum_{j=0}^{N_2-1} \binom{-\frac{1}{2}}{j} \left(\frac{P(x)^\sigma - P(x)^p}{y^{2p}}\right)^j dx$$

Kedlaya in [47], showed an algorithm to compute the zeta function of an hyperelliptic curve and used it to show how to compute the number of points over finite fields. We now show a slight variation of Kedlaya's algorithm which allows to compute the Frobenius matrix.

Algorithm Kedlaya's Algorithm

Input:

- The basis of differentials $\left\{\omega_i = \frac{x^i dx}{y} : i = 0, \ldots, 2g-1\right\}$ of $H^1_{\mathrm{dR}}(C_{\mathbb{Q}_p})$ for a genus g hyperelliptic curve C given by a monic odd degree model, with good reduction at p.
- The desired precision N.

Output:

- The $2g \times 2g$ matrix $\mathbf{M}$ of a p-power lift of Frobenius ϕ
- Functions $h_i \in A^\dagger$ such that $\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$

Description:

1: Compute the working precision N_1 from Proposition 3.30, so that all the computations will be done modulo p^{N_1}.

2: For each i, compute $F_i := \phi^*(\omega_i)$ and group the resulting terms as $\left(\sum p^{k+1} c_{i,j,k}(x) y^j\right) dx/y$, where $c_{i,j,k}(x) \in \mathbb{Z}_p[x]$ have degree $\leq 2g+1$.

3: Compute a list of differentials $d(x^i y^j)$, where $0 \leq i \leq 2g+1$ and j is odd.

4: If F_i has a term $(x^i y^j)dx/y$, with $j < 0$, consider the term $(c_{i,j,k}(x)y^j)dx/y$ with j minimal. Take the unique linear combination of the $d(x^k y^{1+j})$ such that when this linear combination is subtracted from F_i the term $(c_{i,j,k}(x)y^j)dx/y$ cancels off. Re-initialize this as F_i. Do this until F_i no longer has terms of the form $(x^i y^j)dx/y$ with $j < 0$.

5: If F_i has a term $(x^i y^j)dx/y$, with $j \geq 0$, consider the term $(x^m y^j)dx/y$ with $m + j$ maximal. Let $(x^k y^l)dx/y$ be the term such that $d(x^k y^l)$ has highest term $(x^m y^j)dx/y$ and subtract off the appropriate multiple of $d(x^k y^l)$ such that the resulting sum no longer has terms of the form $(x^m y^j)dx/y$ with $j \geq 0$. Re-initialize this as F_i and repeat this process until the resulting F_i is of the form $\left(M_{0,i} + M_{1,i}x + \ldots + M_{2g-1,i}x^{2g-1}\right) dx/y$.

6: For each i, return the expression

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$

Now we are ready to show the Balakrishnan-Bradshaw-Kedlaya algorithm for Coleman integration on hyperelliptic curves.

Algorithm Coleman integration on a hyperelliptic curve [3]

Input:

- A prime $p > 2$ of good reduction for a hyperelliptic curve C.
- Points $P, Q \in C(\mathbb{Q}_p)$ not contained in a Weierstrass residue disk.
- A 1-form ω of the second kind.

Output: The Coleman integral $\int_P^Q \omega$.

Description:

1: Since ω is of the second kind, we may write it as a linear combination of a basis $\{\omega_i : i = 0, \dots, 2g-1\}$ for $H^1_{\mathrm{dR}}(C)$ together with an exact form. Use Kedlaya's algorithm to write $\omega = dh + \sum_{i=0} a_i \omega_i$, which allows us to reduce to the case of Coleman integrals of basis differentials.

2: Use Kedlaya's algorithm to write, for each basis differential ω_i, the expression

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$

3: Using properties of the Coleman integral, we have

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_j \\ \vdots \end{pmatrix} = (\mathbf{M}^t - I)^{-1} \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_j - \int_{\phi(Q)}^Q \omega_j \\ \vdots \end{pmatrix} \tag{3.2}$$

4: Compute $\int_P^Q \omega = h(P) - h(Q) + \sum_{i=0}^{2g-1} a_i \int_P^Q \omega_i$.

Remark 3.31. For the sake of clarity, we explain how to deduce equation 3.2. By property 3 of theorem 3.22, we have

$$\int_{\phi(P)}^{\phi(Q)} \omega_i = \int_P^Q \phi^*\omega_i$$

Using Kedlaya's algorithm we can rewrite the RHS as

$$\begin{aligned} \int_P^Q \phi^*\omega_i &= \int_P^Q \left(dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j \right) \\ &= \int_P^Q dh_i + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j = h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j \end{aligned}$$

By property 2 of theorem 3.22, we get

$$\int_P^Q \omega_i = \int_P^{\phi(P)} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_i + \int_{\phi(Q)}^Q \omega_i = \int_P^{\phi(P)} \omega_i + \int_{\phi(Q)}^Q \omega_i + h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ji} \int_P^Q \omega_j$$

Now, P and $\phi(P)$ are in the same residue disk, so $\int_P^{\phi(P)} \omega_i$ is a tiny integral, which is computable via its power series expansion. The h_i are give by the Kedlaya algorithm

and we can evaluate them on P and Q. Now, equation 3.2 follows from the equation above after using linear algebra to rearrange the terms.

Notice that $\mathbf{M}^t - I$ is invertible since, by the Weil conjectures, the eigenvalues of $\mathbf{M}$ have norm $\sqrt{p} \neq 1$. This proves that the RHS of equation 3.2 is easily computable.

Remark 3.32. For Weierstrass residue disks, because of overconvergence, the lift of Frobenius is only defined near the boundary of the residue disk. So if W is a Weierstrass point and we want to compute $\int_W^P \omega_i$, we choose a point S close to the boundary of the Weierstrass disk of W and decompose the integral as

$$\int_W^P \omega_i = \int_W^S \omega_i + \int_S^P \omega_i$$

The term $\int_W^S \omega_i$ is a tiny integral and the term $\int_S^P \omega_i$ can be computed as above. However, this is computationally hard, because we have to work over a totally ramified extension of $\mathbb{Q}_p$ to compute the integral.

Example 3.33. In Example 3.1 we studied the rational points on the genus 2 hyperelliptic curve

$$\mathcal{C} : y^2 = x^5 - 2x^3 + x + \frac{1}{4}$$

Recall that we have at least 7 rational points:

$$\mathcal{C}(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$$

We also computed an annihilating differential over $\mathbb{Q}_3$

$$\eta = \alpha\omega_0 - \beta\omega_1$$

where

$$\omega_0 = \frac{dx}{2y} \qquad \omega_1 = \frac{xdx}{2y}$$

$$\beta := \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 = 3 + 3^2 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^{10} + O(3^{11})$$

$$\alpha := \int_{(0,1/2)}^{(-1,-1/2)} \omega_1 = 2 + 2 \cdot 3 + 2 \cdot 3^3 + 3^4 + 3^6 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10})$$

We didn't say anything about how `Magma` actually computed those values, but now we can say that it is just an application of the Balakrishnan-Bradshaw-Kedlaya algorithm.

As we said before, we want to compute the set

$$\mathcal{C}(\mathbb{Q}_3)_1 := \left\{ z \in \mathcal{C}(\mathbb{Q}_3) : \int_{(0,1/2)}^{z} \eta = 0 \right\} \supseteq \mathcal{C}(\mathbb{Q})$$

To do that we need to compute the "indefinite" Coleman integrals

$$\int_{(0,1/2)}^{P_t} \eta$$

where P_t ranges over all residue disks, and then find all the $z \in \mathcal{C}(\mathbb{Q}_3)$ such that $\int_{(0,1/2)}^{z} \eta = 0$.
In order to compute these integrals we can choose a lift Q of an $\mathbb{F}_3$-point in the same residue disk ad P_t and then write

$$\int_{(0,1/2)}^{P_t} \eta = \int_{(0,1/2)}^{Q} \eta + \int_{Q}^{P_t} \eta$$

The first integral is just a 3-adic constant, while the second is a tiny integral which we can compute using a local coordinate at Q and integrating the resulting power series. However, since each residue disk contains at least one rational point, we can take Q as that point, in such a way that $\int_{(0,1/2)}^{Q} \eta = 0$, by construction of the annihilating differential. Moreover, since the hyperelliptic involution i is a bijection on $\mathcal{C}(\mathbb{Q})$, we only need to consider the residue disk of Q and not the disk of $i(Q)$, cutting the computations in half.

So we need to compute the Coleman integrals $\int_{(0,1/2)}^{P_t} \eta = \int_{Q}^{P_t} \eta$ where P_t is in the residue disk of $Q = \infty, (0,1/2), (1,1/2), (-1,1/2)$. For example, if $Q = (1,1/2)$, a local coordinate is given by

$$\begin{aligned} x(t) &= 1 + t + O(t^{20}) \\ y(t) &= \frac{1}{2} + 4t^2 + 8t^3 - 11t^4 - 63t^5 + 24t^6 + 680t^7 + 695t^8 - 7210t^9 - 19881t^{10} + 64544t^{11} \\ &\quad + 374802t^{12} - 301946t^{13} - 5872722t^{14} - 5265422t^{15} + 78467963t^{16} + 210631116t^{17} \\ &\quad - 840861878t^{18} - 4667976084t^{19} + O(t^{20}) \end{aligned}$$

and the power series for $\int_{(0,1/2)}^{P_t} \eta = \int_{Q}^{P_t} \eta$ is

$$\begin{aligned} &(2 + 3 + 2\cdot 3^2 + 3^3 + 2\cdot 3^5 + 3^6 + 2\cdot 3^8 + 3^9 + O(3^{10}))t + (3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^6 + 3^7 + 3^8 + 3^9 + 2\cdot 3^{10} + O(3^{12}))t^2 \\ &+ (2\cdot 3 + 3^2 + 3^5 + 3^7 + 3^8 + 3^{10} + O(3^{11}))t^3 + (3^3 + 3^4 + 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + 2\cdot 3^8 + 3^{12} + O(3^{13}))t^4 \\ &+ (2\cdot 3^4 + 2\cdot 3^7 + 3^8 + 3^9 + 2\cdot 3^{11} + 2\cdot 3^{12} + 2\cdot 3^{13} + O(3^{14}))t^5 + (3^4 + 2\cdot 3^5 + 3^6 + 3^7 + 2\cdot 3^8 + 3^9 + 3^{11} + 3^{12} + O(3^{14}))t^6 \\ &+ (2\cdot 3^6 + 2\cdot 3^7 + 3^8 + 3^{10} + 2\cdot 3^{11} + 3^{12} + 2\cdot 3^{14} + O(3^{16}))t^7 + (2\cdot 3^8 + 2\cdot 3^9 + 3^{11} + 3^{12} + 2\cdot 3^{14} + 2\cdot 3^{15} + 2\cdot 3^{16} + O(3^{18}))t^8 \\ &+ (2\cdot 3^6 + 2\cdot 3^9 + 2\cdot 3^{10} + 3^{12} + 2\cdot 3^{14} + 2\cdot 3^{15} + O(3^{16}))t^9 + (2\cdot 3^9 + 3^{10} + 2\cdot 3^{11} + 3^{13} + 3^{16} + 3^{17} + O(3^{19}))t^{10} + \dots \end{aligned}$$

Strassman's theorem implies that it only has one simple zero, namely $t = 0$, which corresponds to the point $(1,1/2)$. Similarly, the same argument shows that for each Q, the power series has only one simple zero, which corresponds to the point Q, and therefore

$$\mathcal{C}(\mathbb{Q}_3)_1 = \mathcal{C}(\mathbb{Q})_{\text{known}} = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$$

This proves that

$$\mathcal{C}(\mathbb{Q}) = \{\infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2)\}$$

Now we want to show how to compute Coleman integrals on general curves. In order to do this we need to generalize Kedlaya's algorithm to compute the action

of Frobenius on general curves. This generalization is given by Tuitman's algorithm ([75, 76]), which computes efficiently the action of Frobenius on rigid cohomology on smooth curves, by using a plane model with a map to $\mathbb{P}^1$. In particular, we will follow the exposition given in [9] and in [8].

Let $\mathcal{C}$ be a smooth, projective and geometrically irreducible curve over $\mathbb{Q}$ of genus g, birational to

$$Q(x,y) = y^{d_x} + Q_{d_x-1}(x)y^{d_x-1} + \ldots + Q_0(x) = 0$$

where $Q_i(x) \in \mathbb{Z}[x]$ for every $i = 0, \ldots, d_x - 1$, such that $Q(x,y)$ is irreducible. The idea of Tuitman's algorithm is the following

1. Consider the map $x : \mathcal{C} \to \mathbb{P}^1$, and remove the ramification locus $r(x)$ of x (this is similar to removing the Weierstrass points in Kedlaya's algorithm).

2. Choose a lift ϕ of the p-power Frobenius in such a way that $x \mapsto x^p$ and then compute the image of y via Hensel lifting.

3. Compute the action of Frobenius on differentials and reduce pole orders using relations in cohomology via Lauder's fibration algorithm

4. Finally, given a basis $\{\omega_i : i = 0, \ldots, 2g-1\}$ of $H^1_{rig}(\mathcal{C} \otimes \mathbb{Q}_p)$, we compute

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$

Let $\Delta(x) \in \mathbb{Z}[x]$ be the discriminant of Q with respect to y and define

$$r(x) = \frac{\Delta(x)}{\gcd(\Delta(x), \Delta'(x)}$$

so that $r(x)$ is squarefree and divides $\Delta(x)$. We also define

$$R = \mathbb{Z}_p\langle x, 1/r, y\rangle/(Q) \qquad R^\dagger = \mathbb{Z}_p\langle x, 1/r, y\rangle^\dagger/(Q)$$

where $\langle\bullet\rangle^\dagger$ stands for the ring of overconvergent functions given by the weak completion of the corresponding polynomial ring. A Frobenius lift $\phi : R^\dagger \to R^\dagger$ is defined as a continuous ring homomorphism that reduces to the p-th power Frobenius map modulo p.

Theorem 3.34. *There exists a Frobenius lift $\phi : R^\dagger \to R^\dagger$ for which $\phi(x) = x^p$.*

Proof. See [76, Thm. 2.6]. □

Definition 3.35. For a point P on a smooth curve, we let ord_P denote the corresponding discrete valuation on the function field of the curve. In particular, ord_0 and ord_∞ are the discrete valuations on the rational function field $\mathbb{Q}(x)$ corresponding to the points 0 and ∞ on $\mathbb{P}^1(\mathbb{Q})$. We extend these definitions to matrices by taking the minimum over their entries.

Definition 3.36. Let $W^0 \in \mathrm{GL}_{d_x}(\mathbb{Q}[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbb{Q}[x, 1/x, 1/r])$ be matrices such that, if we denote

$$b_j^0 = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i \qquad \text{and} \qquad b_j^\infty = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$$

for each $j = 0, \ldots, d_x - 1$, then

- $\left\{b_0^0, \ldots, b_{d_x-1}^0\right\}$ is an integral basis for $\mathbb{Q}(\mathcal{C})$ over $\mathbb{Q}[x]$.
- $\left\{b_0^\infty, \ldots, b_{d_x-1}^\infty\right\}$ is an integral basis for $\mathbb{Q}(\mathcal{C})$ over $\mathbb{Q}[1/x]$.

where $\mathbb{Q}(\mathcal{C})$ is the function field of $\mathcal{C}$. Furthermore, we define $W \in \mathrm{GL}_{d_x}(\mathbb{Q}[x, 1/x])$ to be the change of basis matrix, i.e. $W = (W^0)^{-1} W^\infty$.

Example 3.37. Let $\mathcal{C}/\mathbb{Q}$ be a hyperelliptic curve of genus g with an odd degree monic plane model

$$\mathcal{C} : Q(x, y) = y^2 - f(x) = 0$$

Then we have that $r(x) = f(x)$ and

$$W^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad W^\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1/x^{g+1} \end{pmatrix}$$

In other words, $\{1, y\}$ and $\left\{1, y/x^{g+1}\right\}$ are integral bases for $\mathbb{Q}(\mathcal{C})$ over $\mathbb{Q}[x]$ and $\mathbb{Q}[1/x]$, respectively.

Definition 3.38. We say that the triple (Q, W^0, W^∞) has good reduction at a prime p if the following conditions are satisfied:

1. The discriminant of $r(x)$ is in $\mathbb{Z}_p^\times$.
2. If we define $\mathbb{F}_p(x, y) := \mathrm{Frac}(\mathbb{F}_p[x, y]/(Q))$, then:
   - The reduction modulo p of $\left\{b_0^0, \ldots, b_{d_x-1}^0\right\}$ is an integral basis for $\mathbb{F}_p(x, y)$ over $\mathbb{F}_p[x]$.
   - The reduction modulo p of $\left\{b_0^\infty, \ldots, b_{d_x-1}^\infty\right\}$ is an integral basis for $\mathbb{F}_p(x, y)$ over $\mathbb{F}_p[1/x]$.
3. $W^0 \in \mathrm{GL}_{d_x}(\mathbb{Z}_p[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbb{Z}_p[x, 1/x, 1/r])$.
4. Let

$$\mathcal{R}^0 = \mathbb{Z}_p[x]\, b_0^0 + \ldots + \mathbb{Z}_p[x]\, b_{d_x-1}^0$$
$$\mathcal{R}^\infty = \mathbb{Z}_p[1/x]\, b_0^\infty + \ldots + \mathbb{Z}_p[1/x]\, b_{d_x-1}^\infty$$

   then the discriminants of the finite $\mathbb{Z}_p$-algebras $\mathcal{R}^0/(r(x))$ $\mathcal{R}^\infty/(1/x)$ are invertible in $\mathbb{Z}_p$.

Definition 3.39. We say that a point in $\mathcal{C}^{an}$ is *very infinite* if its x-coordinate is ∞ and *very bad* if it is either very infinite or its x-coordinate is a zero of $r(x)$.

Definition 3.40. We say that a residue disk (and any point inside it) in *infinite* or *bad* if it contains a very infinite or a very bad point, respectively. A point or residue disk is called *finite* if it is not infinite and *good* if it is not bad. Let U be the complement of the very bad points in $\mathcal{C}^{an}$.

From the assumption that (Q, W^0, W^∞) has good reduction at p, it follows that the rigid cohomology spaces $H^1_{rig}(U \otimes \mathbb{Q}_p)$ and $H^1_{rig}(\mathcal{C} \otimes \mathbb{Q}_p)$ are isomorphic to their algebraic de Rham counterparts (see [10]).

Proposition 3.41. *There are p-adically integral 1-forms on U (see [75, 76] for an algorithm), $\omega_0, \ldots, \omega_{2g-1}$, such that:*

1. *$\omega_0, \ldots, \omega_{g-1}$ is a basis for $H^0(\mathcal{C}_{\mathbb{Q}_P}, \Omega^1)$.*
2. *$\omega_0, \ldots, \omega_{2g-1}$ is a basis for $H^1_{rig}(\mathcal{C} \otimes \mathbb{Q}_P)$.*
3. *$ord_P(\omega_i) \geq -1$ for all i, at all finite very bad points P.*
4. *$ord_P(\omega_i) \geq -1 + (ord_0(W) + 1)e_P$ for all i, at all very infinite points P (e_P is the ramification index of P).*

Definition 3.42. The p-power Frobenius ϕ acts on $H^1_{rig}(\mathcal{C} \otimes \mathbb{Q}_p)$, so that there exist a matrix $\mathbf{M} \in \mathbb{Q}_p^{2g \times 2g}$ and functions $h_0, \ldots, h_{2g-1} \in R^\dagger \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$

for $i = 0, \ldots, 2g-1$, where the ω_i are the 1-form described in the previous Proposition.

This implies that we can compute the action of Frobenius on a general 1-form, but after that we need to reduce the pole order using relations in cohomology, much like what we did with Lemmas 3.25 and 3.26. Tuitman's algorithm uses Lauder's fibration algorithm, but we will not go into detail, instead we directly state the following lemmas.

Lemma 3.43. *Let r' denote dr/dx for points not over infinity. For all $n \in \mathbb{N}$ and for every vector $w \in \mathbb{Q}_p[x]^{\oplus d_x}$, there exist vectors $u, v \in \mathbb{Q}_p[x]^{\oplus d_x}$ such that $\deg(v) < \deg(r)$ and*

$$\frac{\sum_{i=0}^{d_x-1} w_i b_i^0}{r^n}\frac{dx}{r} = d\left(\frac{\sum_{i=0}^{d_x-1} v_i b_i^0}{r^n}\right) + \frac{\sum_{i=0}^{d_x-1} u_i b_i^0}{r^{n-1}}\frac{dx}{r}$$

Lemma 3.44. *For every vector $w \in \mathbb{Q}_p[x, 1/x]^{\oplus d_x}$ with $ord_\infty(w) \leq -\deg(r)$, there exist vectors $u, v \in \mathbb{Q}_p[x, 1/x]^{\oplus d_x}$ such that $ord_\infty(u) > ord_\infty(w)$ and*

$$\left(\sum_{i=0}^{d_x-1} w_i b_i^\infty\right)\frac{dx}{r} = d\left(\sum_{i=0}^{d_x-1} v_i b_i^\infty\right) + \left(\sum_{i=0}^{d_x-1} u_i b_i^\infty\right)\frac{dx}{r}$$

Algorithm Tuitman's Algorithm [75, 76]

Input:

- A prime $p > 2$ of good reduction (in the sense of definition 3.38) for a smooth, projective and geometrically irreducible curve $\mathcal{C}/\mathbb{Q}$
- A basis $\left\{\omega_i = \frac{x^i dx}{y} : i = 0, \ldots, 2g-1\right\}$ of $H^1_{rig}(\mathcal{C} \otimes \mathbb{Q}_p)$.

Output: The $2g \times 2g$ $\mathbb{Q}_p$-matrix $\mathbf{M}$ and overconvergent functions $h_i \in R^\dagger \otimes \mathbb{Q}_p$ such that $\phi^*(\omega_i) = dh_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$

Description:

1: Compute the Frobenius lift ϕ: set $\phi(x) = x^p$ and determine $\phi(1/x) \in \mathbb{Z}_p\langle x, 1/r\rangle^\dagger$, $\phi(y) \in R^\dagger$ by Hensel lifting.

2: Finite pole reduction: for $i = 0, \ldots, 2g-1$, find $h_{i,0} \in R \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + G_i\left(\frac{dx}{r(x)}\right)$$

where $G_i \in R \otimes \mathbb{Q}_p$ has poles only at very infinite points.

3: Infinite pole reduction: for $i = 0, \ldots, 2g-1$, find $h_{i,\infty} \in R^\dagger \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + dh_{i,\infty} + H_i\left(\frac{dx}{r(x)}\right)$$

where $H_i \in R \otimes \mathbb{Q}_p$ has poles only at very infinite points and satisfies

$$\mathrm{ord}_P(H_i) \geq (\mathrm{ord}_0(W) - \deg(r) + 2)e_P$$

4: Final reduction: for $i = 0, \ldots, 2g-1$, find $h_{i,end} \in R \otimes \mathbb{Q}_p$ such that

$$\phi^*(\omega_i) = dh_{i,0} + dh_{i,\infty} + dh_{i,end} + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$

where $\mathbf{M} \in \mathbb{Q}_p^{2g\times 2g}$ is the matrix of ϕ^* on $H^1_{rig}(U \otimes \mathbb{Q}_p)$ with respect to the basis $\{\omega_i = \frac{x^i dx}{y} : i = 0, \ldots, 2g-1\}$.

5: For each $i = 0, \ldots, 2g-1$ compute the functions $h_i := h_{i,0} + h_{i,\infty} + h_{i,end}$.

Algorithm Coleman integration on a plane curve [9]

Input:

- A prime $p > 2$ of good reduction (in the sense of definition 3.38) for a smooth, projective and geometrically irreducible curve $\mathcal{C}/\mathbb{Q}$.
- Points $P, Q \in C(\mathbb{Q}_p)$ not contained in very bad residue disks.
- A 1-form ω of the second kind.

Output: The Coleman integral $\int_P^Q \omega$.

Description:

1: Since ω is of the second kind, we may write it as a linear combination of a basis $\{\omega_i : i = 0, \dots, 2g-1\}$ for $H^1_{rig}(\mathcal{C} \otimes \mathbb{Q}_p)$ together with an exact form. Use Tuitman's algorithm to write $\omega = dh + \sum_{i=0} a_i \omega_i$, which allows us to reduce to the case of Coleman integrals of basis differentials.

2: Use Tuitman's algorithm to compute the matrix $\mathbf{M}$ and the functions $h_0, \dots, h_{2g-1}$.

3: Compute the integrals $\int_P^{\phi(P)} \omega_i$ and $\int_{\phi(Q)}^Q \omega_i$, for $i = 0, \dots, 2g-1$, using local coordinates and tiny integrals.

4: Compute $h_i(P) - h_i(Q)$ for $i = 0, \dots, 2g-1$ and use the system of linear equations

$$\sum_{j=0}^{2g-1} (M_j i - \delta_{ij}) \int_P^Q \omega_j = h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i$$

to solve for the $\int_P^Q \omega_i$.

Remark 3.45. The case of points in a very bad disk is analogous to the case of Weierstrass points on a hyperelliptic curve, and it can be treated similarly. Let B a very bad point and B' a point near the boundary of the residue disk of B, then split up the integral

$$\int_B^Q \omega = \int_B^{B'} \omega + \int_{B'}^Q \omega$$

The integral $\int_B^{B'} \omega$ is a tiny integral and $\int_{B'}^Q \omega$ can be computed with the previous algorithm.

Chapter 4

Generalizations

So far, we only dealt with the case in which $r < g$, where $r = \mathrm{rank}(J(\mathbb{Q}))$ and g is the genus of the curve that we are studying. So it is natural to ask what happens if $r \geq g$. The Chabauty-Coleman method no longer works, but Faltings' theorem implies that the curve has still a finite number of rational points.

In this chapter we want to talk about some generalizations of the classical Chabauty-Coleman method which can be applied even when $r \geq g$. In particular, some of these form an active area of research.

4.1 Elliptic Chabauty

The elliptic Chabauty method works by transforming the problem of finding the rational points on a curve into the problem of finding points on certain elliptic curves over number fields with x-coordinate in $\mathbb{Q}$. This works particularly well if $r = g$.

Let E be an elliptic curve defined by the equation

$$E : y^2 = a_0x^3 + a_2x^2 + a_4x + a_6$$

over a number field $\mathbb{Q}(\alpha)$ of degree d with $a_0 \neq 0$. As we said before the aim of this method is to find all points $(x, y) \in E(\mathbb{Q}(\alpha))$ such that $x \in \mathbb{Q}$. Following Chapter 4 of [68], we recall that the change of variables $z = -\frac{x}{y}, w = -\frac{1}{y}$ allows us to define a formal group law on E. In other words, if $P_1 = (z_1, w_1), P_2 = (z_2, w_2) \in E$, then the z-coordinate of $P_1 + P_2$ can be written as a formal series in z_1, z_2 with coefficients in $\mathbb{Z}[a_0, a_2, a_4, a_6]$ and we will write $z(P_1 + P_2) = \mathcal{F}(z_1, z_2) \in \mathbb{Z}[a_0, a_2, a_4, a_6][[z_1, z_2]]$. In the same chapter it is also described the construction of the formal logarithm and the formal exponential, i.e. formal series with coefficients in $\mathbb{Q}[a_0, a_2, a_4, a_6]$ such that

$$\mathrm{Log} \circ \mathrm{Exp}(T) = \mathrm{Exp} \circ \mathrm{Log}(T) = T$$

$$\mathrm{Log}(\mathcal{F}(z_1, z_2)) = \mathrm{Log}(z_1) + \mathrm{Log}(z_2)$$

$$\mathcal{F}(\mathrm{Exp}(z_1), \mathrm{Exp}(z_2)) = \mathrm{Exp}(z_1 + z_2)$$

By writing the w-coordinate as a formal series in z, we can also write the inverse of the x-coordinate of a point $P = (z, w) \in E(\mathbb{Q}(\alpha))$ as a formal series $\Phi \in \mathbb{Z}[a_0, a_2, a_4, a_6][[z]]$ and, similarly, the x-coordinate of the sum of P with the point $(x_0, y_0) \in E(\mathbb{Q}(\alpha))$ as a formal series $\Psi \in \mathbb{Z}[a_0, a_2, a_4, a_6, x_0, y_0][[z]]$:

$$\Phi(z) = a_0(z^2 + a_2 z^4 + (a_4 a_0 + a_2^2)z^6) + O(z^8)$$

$$\Psi_{(x_0,y_0)}(z) = x_0 + 2y_0 z + (3a_0 x_0^2 + 2a_2 x_0 + a_4)z^2 + (4a_0 x_0 y_0 + 2a_2 y_0)z^3 + O(z^4)$$

We will assume that the rank of $E(\mathbb{Q}(\alpha))$ is non zero (the case of rank 0 is trivial) and that it is strictly less than $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. This is the analogue of the condition on the rank of the Jacobian in the classical Chabauty method. We will also suppose that the structure of the Mordell-Weil group $E(\mathbb{Q}(\alpha))$ is known, i.e.

$$E(\mathbb{Q}(\alpha)) = E(\mathbb{Q}(\alpha))_{tors} \oplus P_1\mathbb{Z} \oplus \ldots \oplus P_r\mathbb{Z}$$

Now consider an odd prime p which satisfies the following conditions (here, $\widetilde{-}$ is the reduction modulo p):

1. $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = d$
2. p is not ramified in $\mathbb{Q}(\alpha)$
3. $|\alpha|_p = 1$
4. The residue field of $\mathbb{Q}_p(\alpha)$ is $\mathbb{F}_p(\widetilde{\alpha})$
5. E has good reduction in p
6. $|a_i|_p \leq 1$, for $i = 0, 2, 4, 6$

The first condition is the most difficult to realize. As a matter of fact, it is always verified if $d = 2$ or 3 but, for example, it is not possible in biquadratic fields. However, sometimes one can work around this condition as Flynn and Wetherell did in [40]. The meaning of conditions 3 and 4 is that α (and its reduction) must be a generator of every ring of integers we need to consider.

In light of condition 5, the reduction $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p(\widetilde{\alpha})$. Then, we can define for every $i = 1, \ldots, r$, m_i as the order of $\widetilde{P_i}$ in $\widetilde{E}(F_p(\widetilde{\alpha}))$ and $Q_i = m_i P_i \in E(\mathbb{Q}(\alpha))$ so that Q_i is in the kernel of the reduction for every i.

Define the finite set

$$\mathcal{U} = \left\{ T + k_1 P_1 + \ldots + k_r P_r : T \in E(\mathbb{Q}(\alpha)), \left\lfloor -\frac{m_i}{2} \right\rfloor + 1 \leq k_i \leq \left\lfloor \frac{m_i}{2} \right\rfloor \right\}$$

Then every point $P \in E(\mathbb{Q}(\alpha))$ can be uniquely written as

$$P = U + n_1 Q_1 + \ldots + n_r Q_r$$

where $U \in \mathcal{U}$ and $n_1, \ldots, n_r \in \mathbb{Z}$.

Now, we want to write the x-coordinate of P as a formal series in $n_1, \ldots, n_r$ using the formal series that we saw above. For example, by using the formal logarithm and exponential we can easily see that the z-coordinate of $n_1Q_1 + \ldots + n_rQ_r$ can be written as a formal series in $n_1, \ldots, n_r$, as

$$z(n_1Q_1 + \ldots + n_rQ_r) = \mathrm{Exp}(n_1\mathrm{Log}(z(Q_1)) + \ldots + n_r\mathrm{Log}(z(Q_r)))$$

in particular, condition 6 and the fact that the points Q_i are in the kernel of the reduction map, imply that the coefficient of $n_1^{e_1} \ldots n_r^{e_r}$ in this formal series is in $\mathbb{Z}_p[\alpha]$ and tend to 0 as $e_1 + \ldots + e_r$ tend to infinity.

In order to write a formal series $\theta_U(n_1, \ldots, n_r)$ for the x-coordinate of P we distinguish two cases. If U is the point at infinity then we have that

$$\theta_U(n_1, \ldots, n_r) = \frac{1}{x(n_1Q_1 + \ldots + n_rQ_r)} = \Phi(n_1Q_1 + \ldots + n_rQ_r) \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]]$$

Otherwise, if U is not the point at infinity, then

$$\theta_U(n_1, \ldots, n_r) = x(U + n_1Q_1 + \ldots + n_rQ_r) = \Psi_U(n_1Q_1 + \ldots + n_rQ_r) \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]]$$

Decompose θ_U into its components as follows

$$\theta_U = \theta_U^{(0)} + \theta_U^{(1)}\alpha + \ldots + \theta_U^{(d-1)}\alpha^{d-1}$$

where each $\theta_U^{(i)} \in \mathbb{Z}_p[[n_1, \ldots, n_r]]$, then the condition on the rationality of $x(P)$ can be written as

$$\theta_U^{(1)}(n_1, \ldots, n_r) = \ldots = \theta_U^{(d-1)}(n_1, \ldots, n_r) = 0 \tag{4.1}$$

Remark 4.1. Now it should be clear why we imposed that the rank r must be strictly less than d. We have $d - 1$ equations in r variables so it should be natural to suppose $r \leq d - 1$.

So we have translated the problem of searching points with rational x-coordinate into the problem of searching for zeros of formal series. If $r = 1$, it suffices to bound the number of zeros of only one of these (univariate) series, so we can apply Strassman's theorem (Theorem 2.16). On the other hand, if $r > 1$, then Flynn and Wetherell [39] suggest applying a version of Weierstrass' preparation theorem in several variables in order to reduce to the previous case.

Finally, suppose that we have a bound on the number of zeros of Equation 4.1 for every $U \in \mathcal{U}$, this yields a bound on the number of points of the form $U + n_1Q_1 + \ldots + n_rQ_r$ for a fixed U with rational x-coordinates. Summing over the (finitely many) $U \in \mathcal{U}$ yields a bound on the number of points in $E(\mathbb{Q}(\alpha))$ with x-coordinate in $\mathbb{Q}$.

The main problem with this argument is that it only gives us a bound on the number of points without giving the point explicitly. In general, this bound is usually sharp and allows us to conclude that there aren't points other than the one already found. However, there could be some obstacles:

- The bound given by Strassman's theorem could be not sharp.
- The Strassman's bound is sharp, but one of the zeros of the formal series could not correspond to a point on the elliptic curve.
- The Strassman's bound is sharp, every p-adic zero of the formal series corresponds to a point on the elliptic curve, but some of those points could be unknown, for example because their height is too large.

Now, we want to describe some techniques for reducing the computation of rational points on a curve to an elliptic Chabauty problem.

4.1.1 How to apply Elliptic Chabauty

We will discuss 3 methods, but the basic principle is always the same: find an abelian variety $\mathcal{A}$ with an isogeny to the Jacobian $J_{\mathcal{C}}$. Now, find a set of embeddings of $\mathcal{C}$ into J and take the preimages of those embeddings by the isogeny; this yields a set of curves on $\mathcal{A}$ such that their rational points cover the set $\mathcal{C}(\mathbb{Q})$.

Covers with isogenies

We start by describing the argument used by Flynn and Wetherell in [39] for biellitpic curves, i.e. curves defined by equation of the following type:

$$\mathcal{C} : Y^2 = G(X^2)$$

where $G(X) \in \mathbb{Z}[X]$ is a degree 3 polynomial, with three distinct roots $\gamma_1, \gamma_2, \gamma_3 \in \overline{\mathbb{Q}}$. This is a curve of genus 2, so if the Mordell-Weil rank of the Jacobian is 0 or 1 we can use Theorem 2.3 and Theorem 2.17 to conclude. So, we will assume that the rank is at least 2.

Define the two maps

$$\begin{aligned} f_1 : \mathcal{C} &\longrightarrow E_1 \\ (X, Y) &\longmapsto (X^2, Y) \\ f_2 : \mathcal{C} &\longrightarrow E_2 \\ (X, Y) &\longmapsto \left(\frac{1}{X^2}, \frac{Y}{X^3}\right) \end{aligned}$$

from $\mathcal{C}$ to the elliptic curves

$$E_1 : Y^2 = G(X) = (X - \gamma_1)(X - \gamma_2)(X - \gamma_3)$$

$$E_2 : y^2 = x^3 G\left(\frac{1}{x}\right) = (1 - \gamma_1 x)(1 - \gamma_2 x)(1 - \gamma_3 x)$$

and let $\mathcal{A} = E_1 \times E_2$. Following chapter 1 of [25], any member of $J(\mathbb{Q})$ may be represented by a divisor of the form $P_1 + P_2 - \infty^+ - \infty^-$, where ∞^+, ∞^- are the two

points at infinity in $\mathcal{C}(\mathbb{Q})$, P_1, P_2 are points on C and either P_1, P_2 are both $\mathbb{Q}$-rational or P_1, P_2 are quadratic over $\mathbb{Q}$ and conjugate. We will denote such a divisor as $\{P_1, P_2\}$. This representation defines a bijection with $J(\mathbb{Q})$, except that everything of the form $\{(x,y),(x,-y)\}$ must be identified into a single point $\mathcal{O}$, which should be seen as the group identity in $J(\mathbb{Q})$.

Then we can find two isogenies

$$\begin{aligned}
\phi : \mathcal{A} &\longrightarrow J \\
\big((X,Y),(x,y)\big) &\longmapsto \left\{(\sqrt{X},Y),(-\sqrt{X},Y)\right\} + \left\{\left(\frac{1}{\sqrt{x}},\frac{y}{x\sqrt{x}}\right),\left(-\frac{1}{\sqrt{x}},-\frac{y}{x\sqrt{x}}\right)\right\} \\
\phi' : J &\longrightarrow \mathcal{A} \\
\{(X_1,Y_1),(X_2,Y_2)\} &\longmapsto \left((X_1^2,Y_1)+(X_2^2,Y_2),\left(\frac{1}{X_1^2},\frac{Y_1}{X_1^3}\right)+\left(\frac{1}{X_2^2},\frac{Y_2}{X_2^3}\right)\right)
\end{aligned}$$

Both their kernels have order 4 and are isomorphic to the Klein 4-group V_4:

$$\ker(\phi) = \left\{\mathcal{O}_1 \times \mathcal{O}_2, (\gamma_1,0)\times\left(\frac{1}{\gamma_1},0\right),(\gamma_2,0)\times\left(\frac{1}{\gamma_2},0\right),(\gamma_3,0)\times\left(\frac{1}{\gamma_3},0\right)\right\}$$

$$\ker(\phi') = \left\{\mathcal{O},\{(\sqrt{\gamma_1},0),(-\sqrt{\gamma_1},0)\},\{(\sqrt{\gamma_2},0),(-\sqrt{\gamma_2},0)\},\{(\sqrt{\gamma_3},0),(-\sqrt{\gamma_3},0)\}\right\}$$

Moreover, their compositions $\phi\circ\phi'$ and $\phi'\circ\phi$ are both multiplication by 2 maps on the respective abelian varieties. As in [61], there is an injective homomorphism

$$\begin{aligned}
\mu : J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q})) &\longrightarrow L_1^\times/(L_1^\times)^2 \times L_2^\times/(L_2^\times)^2 \times L_3^\times/(L_3^\times)^2 \\
\{(X_1,Y_1),(X_2,Y_2)\} &\longmapsto \left[(X_1^2-\gamma_1)(X_2^2-\gamma_1),(X_1^2-\gamma_2)(X_2^2-\gamma_2),(X_1^2-\gamma_3)(X_2^2-\gamma_3)\right]
\end{aligned}$$

where $L_i = \mathbb{Q}(\gamma_i)$.

Since $J(\mathbb{Q})/2J(\mathbb{Q})$ is finite by the weak Mordell-Weil theorem (Theorem 1.51) and $2J(\mathbb{Q}) = \phi\left(\phi'\left(J(\mathbb{Q})\right)\right) \subseteq \phi\left(\mathcal{A}(\mathbb{Q})\right)$ we find that

$$J(\mathbb{Q})/\phi\left(\mathcal{A}(\mathbb{Q})\right) \cong {}^{J(\mathbb{Q})/2J(\mathbb{Q})}\!\!\diagup_{\phi\left(\mathcal{A}(\mathbb{Q})\right)/2J(\mathbb{Q})}$$

is finite as well and can be explicitly determined (for example with a descent). So, suppose that we'd done that:

$$J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q})) = \{D_1,\ldots,D_m\}$$

then for every $(X,Y)\in\mathcal{C}(\mathbb{Q})$ there exists an $i=1,\ldots,m$ such that $\{(X,Y),\infty^+\} = D_i$ in $J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q}))$ and thus $\mu^{(j)}(D_i) = \mu^{(j)}\left(\{(X,Y),\infty^+\}\right)$, which is equivalent to say that $\mu^{(j)}(D_i) = X^2-\gamma_j$ in $L_j^\times/(L_j^\times)^2$.

Since $G(X^2) = Y^2$ is a square, there exists $Y_{i,j}\in L_j$ such that

$$Y_{i,j}^2 = \mu^{(j)}(D_i)\frac{G(X^2)}{X^2-\gamma_j}$$

Multiplying by X^2 both sides and applying the change of variables $y_{i,j} = XY_{i,j}$, $x = X^2$ we get the identity

$$y_{i,j}^2 = \mu^{(j)}(D_i)\frac{xG(x)}{x-\gamma_j}$$

So we get a point $(x, y_{i,j}) \in \mathbb{Q} \times L_j$ on the elliptic curve

$$E_{i,j} : V^2 = \mu^{(j)}(D_i)\frac{WG(W)}{W - \gamma_j}$$

Thus we can use the method outlined above to find those points and therefore the rational points on $\mathcal{C}$.

As an example we solve the only Diophantine equation of genus ≥ 2 in Diophantus' *Arithmetica* (problem VI.17)

Theorem 4.2 (Wetherell, [80, Prop. 5.1.])**.** *The only rational solutions of the equation*

$$y^2 = x^8 + x^4 + x^2$$

are $(0,0)$ *and* $\left(\pm\frac{1}{2}, \pm\frac{9}{16}\right)$.

Proof. By removing the singularity at $(0,0)$ we get the bielliptic curve

$$\mathcal{C} : y^2 = x^6 + x^2 + 1$$

Applying the theory that we developed above we get the elliptic curves

$$E_1 : y^2 = x^3 + x + 1 \qquad \text{and} \qquad E_2 : y^2 = x^3 + x^2 + 1$$

Let $\gamma_1 = \alpha$, where $\alpha^3 + \alpha + 1 = 0$ and note that

$$G(x) = x^3 + x + 1 = (x - \alpha)(x^2 + \alpha x + \alpha^2 - 1)$$

From `Magma` computations we get that $J(\mathbb{Q})$ has rank 2 and it is generated by $\{(0,1),(0,1)\}$ and $\{(0,1),\infty^+\}$. By explicit computations, $\phi\left(((0,1),\mathcal{O}_2)\right) = \{(0,1),(0,1)\}$, hence $\{(0,1),(0,1)\}$ is trivial in $J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q}))$; moreover $\mu\left(\{(0,1),\infty^+\}\right) \neq [1,1,1]$ but

$$\mu\left(2\left\{(0,1),\infty^+\right\}\right) = \mu\left(\left\{(0,1),\infty^+\right\}\right)^2 = [1,1,1]$$

so, since μ is injective, we have that $\{(0,1),\infty^+\}$ is a point of exact order 2 in $J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q}))$. Therefore we conclude that

$$J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q})) = \{D_1 = \mathcal{O}, D_2 = \left\{(0,1),\infty^+\right\}\}$$

Now, for every $(X,Y) \in \mathcal{C}(\mathbb{Q})$ we must have $\{(X,Y),\infty^+\} = D_1$ or D_2 in $J(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q}))$ so $x = X^2 \in \mathbb{Q}$ must satisfy one of the equations

$$E_{1,1} : y_{1,1}^2 = x(x^2 + \alpha x + \alpha^2 - 1)$$

$$E_{2,1} : y_{2,1}^2 = -\alpha x(x^2 + \alpha x + \alpha^2 - 1)$$

By using `Magma` we find that $E_{1,1}(\mathbb{Q}(\alpha)) = \langle(0,0)\rangle \oplus (-\alpha, 1)\mathbb{Z}$ (the point $(0,0)$ has order 2) and $E_{2,1}(\mathbb{Q}(\alpha)) = \{\mathcal{O}, (0,0)\}$.

So we will work only on $E_{1,1}$. Using the same notations as above, let $P_1 = (-\alpha, 1)$ and use $p = 5$. We can take $m_1 = 28$, i.e. $28P_1$ is in the kernel of the reduction modulo

5, however it is more efficient to take $Q_1 = 14P_1 + (0,0)$ which is also int the kernel of the reduction modulo 5. So we have

$$\mathcal{U} = \{kP_1 : -6 \leq k \leq 7\} \cup \{(0,0) + kP_1 : -6 \leq k \leq 7\}$$

in this way, every $P \in E_{1,1}(\mathbb{Q}(\alpha))$ can be written uniquely as $P = U + nQ_1$, for some $U \in \mathcal{U}$ and $n \in \mathbb{Z}$.

We can compute

$$z(nQ_1) = \mathrm{Exp}(n\mathrm{Log}(z(Q_1))) \equiv 5(21 + 15\alpha + 21\alpha^2)n \pmod{5^3}$$

By using the formulas given above for θ_U in the case $U = -2P_1 = (1/4,\ 1/8 - \alpha/2 + \alpha^2/4)$, we get

$$\theta_{-2P_1}(n) \equiv 94 + 5(17\alpha + 9\alpha^2)n + 5^2(2 + \alpha + \alpha^2)n^2 \pmod{5^3}$$

We apply Strassman's theorem on $\theta^{(2)}_{-2P_1}(n) \equiv 45n + 25n^2 \pmod{5^3}$ and we deduce that $\theta^{(2)}_{-2P_1}(n)$ has at most one root. However, $n = 0$ is a root, since $-2P_1 + 0 \cdot Q_1$ has x-coordinate equal to $1/4 \in \mathbb{Q}$, hence $n = 0$ is the only solution.

Similarly, the same argument implies that for $U = \mathcal{O}, (0,0), 2P_1$, $n = 0$ is the only value such that $U + nQ_1$ has rational x-coordinate.

For the remaining values of $U \in \mathcal{U}$, we can show that the constant term of $\theta^{(2)}_U(n)$ has 5-adic absolute value strictly greater than all the other terms, so we have no roots in these cases.

This proves that the only points in $E_{1,1}(\mathbb{Q}(\alpha))$ with rational x-coordinate are $\mathcal{O}, (0,0)$ and $\pm 2P_1 = \pm(1/4, 1/8 - \alpha/2 + \alpha^2/4)$.

Therefore the only rational values that x may assume are $\infty, 0, 1/4$ which imply that $X = \infty, 0, \pm 1/2$. The corresponding points on $\mathcal{C}$ are $\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)$, which correspond to the solutions that we were looking for. □

Covers with multiplication-by-2 maps

Now, we want to generalize the previous argument to more general curves.

Let C be an hyperelliptic curve defined over a number field K, with a known K-rational point mapped to infinity

$$C : y^2 = F(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = F_1(x) \ldots F_k(x)$$

where $a_i \in K$ and $F_1(X), \ldots, F_k(X)$ are the irreducible factors of $F(X)$ over K. For each i, let α_i be a root of $F_i(X)$ and let $L_i = K(\alpha_i)$. When n is even[1], we have to K-rational points $\infty^+, \infty^- \in C(K)$ that lie over the point at infinity on C; while, if n is odd, we have only one such point $\infty^+ \in C(K)$. Define a map q (the analogue of the

[1]If we suppose further that $4 \nmid n$, then every 2-torsion element of $J(K)$ would be represented by a K-rational set of Weierstrass points on C; but we do not need this hypothesis.

map μ in the previous method) on $J(K)$ by

$$q : J(K) \longrightarrow \left(L_1^\times/(L_1^\times)^2 \times \ldots \times L_k^\times/(L_k^\times)^2 \right)/\sim$$
$$\left[\sum_{j=1}^m n_j(x_j, y_j) \right] \longmapsto \left[\prod_{j=1}^m (x_j - \alpha_1)^{n_j}, \ldots, \prod_{j=1}^m (x_j - \alpha_k)^{n_j} \right]$$

where the equivalence relation $\sim$ is defined by

$$n \text{ even: } [a_1, \ldots, a_k] \sim [b_1, \ldots, b_k] \iff a_1 = \lambda b_1, \ldots, a_k = \lambda b_k, \text{ for some } \lambda \in K^\times$$
$$n \text{ odd: } [a_1, \ldots, a_k] \sim [b_1, \ldots, b_k] \iff a_1 = b_1, \ldots, a_k = b_k$$

In the definition of the map q, $x_j - \alpha_i$ should be taken to be 1 when (x_j, y_j) is any point at infinity. Moreover, in both cases the square brackets denote an equivalence class: in the LHS a class of divisors modulo linear equivalence, in the RHS a class k-tuples modulo $\sim$. When n is odd, $\ker(q) = 2J(K)$; while if n is even, then either $\ker(q) = 2J(K)$ or $\ker(q)$ has index 2 in $2J(K)$ (see [60], [69]).

Now suppose that $G(X) \in \overline{K}[X]$ divides $F(X)$, then there is an induced map

$$q_G : J(K) \longrightarrow \left(L_G^\times/(L_G^\times)^2 \right)/\sim$$
$$\left[\sum_{j=1}^m n_j(x_j, y_j) \right] \longmapsto \left[\prod_{j=1}^m G(x_j)^{n_j} \right] \tag{4.2}$$

where L_G denotes the smallest field containing K over which $G(X)$ is defined. As in the previous method, $J(K)/\ker(q)$ is finite and can be computed once $J(K)/2J(K)$ is found, so that we can write

$$J(\mathbb{Q})/\ker(q) = \{D_1, \ldots, D_r\}$$

Let $P = (x_0, y_0) \in C(K)$, then $[P - \infty^+] \in J(K)$ and for some $i = 1, \ldots, r$ we must have $q([P - \infty^+]) = q(D_i)$ and therefore $q_G([P - \infty^+]) = q_G(D_i)$ for every $G(X) \mid F(X)$. In other words,

$$q_G(D_i)G(x_0) \in (L_G^\times)^2 \text{ for all } G(X) \mid F(X)$$

Thus, every choice of G yields an hyperelliptic curve over L_G on which there must be an L_G-rational point with K-rational x-coordinate. We define $\mathcal{B}_i$ to be the curve defined by all (or some) of these equations

$$\mathcal{B}_i = \{v_{i,G}^2 = q_G(D_i)G(x) : G(X) \mid F(X)\}$$

So, in order to determine all points $P \in C(K)$ is sufficient to find all points on $\mathcal{B}_i$ with $x \in K$, $v_{i,G} \in L_G^\times$, for every $i = 1, \ldots, r$. Notice that when $G(X)$ has degree 3 or 4, then $v_{i,G}^2 = q_G(D_i)G(x)$ is potentially an elliptic curve, and if its rank is less than $[L_G : K]$ then we can apply the techniques we saw before. We will use this method in section 5.2 to prove Theorem 5.3.

Using resultants

This last method uses a more classic approach and does not rely on the more complex tools of the previous methods.

Suppose that C is an hyperelliptic curve defined over $\mathbb{Q}$ by

$$C : y^2 = F(x) = F_1(x)F_2(x)$$

where $F(X) \in \mathbb{Q}[X]$ is square-free, $F_1(X), F_2(X) \in K[X]$, K is a number field, $\deg(F) \geq 6$ and $\deg(F_1) = 3$ or 4. Suppose that K has class number 1 and let $(x_0, y_0) \in C(\mathbb{Q})$. Then, there are $y_1, y_2, \alpha \in K$ such that

$$\alpha y_1^2 = F_1(x_0) \qquad \text{and} \qquad \alpha y_2^2 = F_2(x_0)$$

It is clear that we can choose α to be square-free. Moreover, we can prove that α must divide the resultant of the polynomials $F_1(X)$ and $F_2(X)$, so that we have only a finite number of possible values for α. Hence we find a finite number of elliptic curves over K with equations

$$E_\alpha : y^2 = \alpha F_1(x)$$

and notice that $(x_0, \pm\alpha y_1) \in E_\alpha(K)$ has $\mathbb{Q}$-rational x-coordinate. So the problem of finding $C(\mathbb{Q})$ can again be reduced to the problem of finding points of $E_\alpha(K)$ with x-coordinate in $\mathbb{Q}$, which we already know how to do. We will apply those ideas in section 5.3 and in the following paragraph.

4.1.2 An explicit example

We said above that we can use Strassman's theorem in order to apply elliptic Chabauty when the resulting elliptic curves have rank 1. So we want to show what we can do when the rank is larger, and we will do it by proving the following result (taken from [32]).

Theorem 4.3. *Let C be the hyperelliptic curve over $\mathbb{Q}$ defined by the equation*

$$C : y^2 = F(x) = x^9 - 6x^8 + 31x^7 - 81x^6 + 177x^5 - 176x^4 - 9x^3 + 107x^2 + 19x + 1$$

Then $C(\mathbb{Q}) = \{\infty, (1, \pm 8), (0, \pm 1)\}$.

Clearly C has genus $\frac{9-1}{2} = 4$ and we using `Magma` we can find that the rank of $J(\mathbb{Q})$ is 4, so we cannot use Chabauty's theorem directly.

Let $K = \mathbb{Q}(\beta)$, where β is a zero of $x^3 + 2x + 1$; then $F(X)$ factorizes over K with irreducible factors:

$$\begin{aligned} F_1(X) &= X^3 - 2X^2 + (-4\beta^2 - \beta + 1)X + 1 \\ F_2(X) &= X^6 - 4X^5 + (4\beta^2 + \beta + 22)X^4 + (-8\beta^2 - 2\beta - 34)X^3 + \\ &\quad + (37\beta^2 - 15\beta + 83)X^2 + (4\beta^2 + \beta + 18)X + 1 \end{aligned}$$

We saw above that if $(x_0, y_0) \in C(\mathbb{Q})$, then there exists $y_1 \in K$ such that $(x_0, y_1) \in E(K)$, where E is the elliptic curve

$$E : y^2 = F_1(x) = x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1$$

which has Mordell-Weil rank 2 over K, thus we can apply the elliptic Chabauty method. However, in order to do this, we have to bound the number of p-adic zeros of a system of two formal series in two variables. This can be done by using a generalization of Strassman's theorem which relies on a version of Weierstrass' preparation theorem.

An explicit Weierstrass' preparation theorem in 2 variables

Define, like in definition 3.3, the ring

$$\mathbb{Z}_p\langle x_1, x_2\rangle := \left\{ \sum_{i,j\geq 0} a_{i,j} x_1^i x_2^j : a_{i,j} \in \mathbb{Z}_p, \lim_{i+j\to\infty} |a_{i,j}|_p = 0 \right\}$$

and recall the definition of the Gauss norm (see remark 3.8) on $\mathbb{Z}_p\langle x_1, x_2\rangle$:

$$\|f\| = \max_{i,j\geq 0} |a_{i,j}|_p$$

Similarly, we can define $\mathbb{Z}_p\langle x_2\rangle$ and equip it with the Gauss norm, which we will denote by $\|\cdot\|_1$. Now, it is easy to define the set $\mathbb{Z}_p\langle x_2\rangle\langle x_1\rangle$ as the subset of $\mathbb{Z}_p\langle x_2\rangle\,[[x_1]]$ in which the norm of the coefficients tends to 0 in $\mathbb{Z}_p\langle x_2\rangle$.

Then we identify $\mathbb{Z}_p\langle x_2\rangle\langle x_1\rangle$ with $\mathbb{Z}_p\langle x_1, x_2\rangle$, since for every $f \in \mathbb{Z}_p\langle x_1, x_2\rangle$ we can write

$$f = \sum_{i=0}^{\infty} f_i x_1^i$$

where $f_i \in \mathbb{Z}_p\langle x_2\rangle$ and $\|f_i\|_1 \to 0$ when $i \to \infty$.

It is easy to show that $f \in \mathbb{Z}_p\langle x_2\rangle$ is invertible if and only if $|a_0|_p = 1$ and $|a_i|_p < 1$ for every $i > 0$ and, similarly, $f \in \mathbb{Z}_p\langle x_1, x_2\rangle$ is invertible if and only if $|a_{0,0}|_p = 1$ and $|a_{i,j}|_p < 1$ for every $(i, j) \neq (0, 0)$.

Finally, $f = \sum_{i=0}^{\infty} f_i x_1^i \in \mathbb{Z}_p\langle x_2\rangle\langle x_1\rangle$ is called *general* in x_1 of order s if $f_s \in \mathbb{Z}_p\langle x_2\rangle^\times$ and $\|f_i\|_1 < 1$ for every $i > s$.

Theorem 4.4 (Sugatani [72]). *Let $f \in \mathbb{Z}_p\langle x_1, x_2\rangle$, general in x_1 of order s. Then, there exist unique functions $h, g_0, \ldots, g_{s-1}, g_s$ such that*

- *$h \in \mathbb{Z}_p\langle x_1, x_2\rangle^\times$ and $h_0(x_2) = 1$.*
- *$g_0, \ldots, g_{s-1} \in \mathbb{Z}_p\langle x_2\rangle$ and $g_s \in \mathbb{Z}_p\langle x_2\rangle^\times$.*
- *$f(x_1, x_2) = h(x_1, x_2) \cdot (g_s(x_2)x_1^s + \ldots + g_1(x_2)x_1 + g_0(x_2))$.*

In order to bound the number of common p-adic zeros of two formal series in two variables, we need a way of finding effectively the functions in the statement of Theorem 4.4. By "effectively", we mean that if f is given with some precision, then we should be able to find $h, g_0, \ldots, g_s$ with the same precision. Let

$$f(x_1, x_2) = \sum_{i,j \geq 0} a_{i,j} x_1^i x_2^j \in \mathbb{Z}_p\langle x_1, x_2 \rangle \tag{4.3}$$

$$g(x_1, x_2) = g_0(x_2) + g_1(x_2)x_1 + \ldots + g_s(x_2)x_1^s \tag{4.4}$$

$$h(x_1, x_2) = 1 + \sum_{i=0}^{\infty} h_n(x_2) x_1^n \tag{4.5}$$

as in Theorem 4.4. Comparing the coefficients of the term x_1^n in the equation

$$f(x_1, x_2) \ = \ h(x_1, x_2)\, g(x_1, x_2)$$

gives

$$h_n(x_2)g_0(x_2) + h_{n-1}(x_2)g_1(x_2) + \ldots + h_{n-s}(x_2)g_s(x_2) = f_n(x_2) \tag{4.6}$$

where we will say that $h_0(x_2) = 1$ and $h_n(x_2) = 0$ if $n < 0$.

Since h is inveritble in $\mathbb{Z}_p\langle x_1, x_2 \rangle$, we know that $\|h_i(x_2)\|_1 < 1$ for every $i \geq 1$. Moreover, as $f_s(x_2)$ is invertible in $\mathbb{Z}_p\langle x_2 \rangle$, equation 4.6 with $n = s$ implies that $g_s(x_2)$ is invertible in $\mathbb{Z}_p\langle x_2 \rangle$. This allows to prove the following result.

Proposition 4.5 (Duquesne [31]). *We can explicitly compute the functions h_i from $g_0, \ldots, g_s$ using the following formula*

$$h_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{g_s^{k+1}} \sum_{i_0 + \ldots + i_{s-1} = k} \binom{k}{i_0, \ldots, i_{s-1}} f_{ind(n,k,s,\mathbf{i})} \prod_{j=0}^{s-1} g_j^{i_j}$$

where

- $\mathbf{i} = (i_0, \ldots, i_{s-1})$;
- $ind(n, k, s, \mathbf{i}) = n + s + \sum_{j=0}^{s-1} (s - j) i_j$;
- $\binom{k}{i_0, \ldots, i_{s-1}} = \dfrac{k!}{i_0! \cdot \ldots \cdot i_{s-1}!}$ *is the multinomial coefficient.*

On the other hand, since we defined $h_0 = 1$ and $h_n = 0$ if $n < 0$, we can use equation 4.6 to derive the following identities:

$$g_0 = f_0$$

$$g_i = f_i - \sum_{j=1}^{i} h_j g_{i-j} \quad \text{for every } 1 \leq i \leq s$$

This allows to compute the formal series g_i by using recursively the formulas above and Proposition 4.5. However these computations may become very challenging, so

we will present a more useful method to compute the functions g_i with the same precision as the f_i.

Suppose that we know the formal series g_i and h_i modulo some power of p (e.g. p^{k_0}), we want to show how we can compute the same series but modulo p^{k_0+1} if we know the formal series f_i modulo p^{k_0+1}.

- First of all, we compute the inverse of g_s modulo p^{k_0}.
- Secondly, we compute the series $h_1, \ldots, h_s$ modulo p^{k_0+1}, using Proposition 4.5. This is possible because the series g_j are known modulo p^{k_0} and the series f_i are known modulo p^{k_0+1} and are divisible by p, so that the products $g_j f_i$ are computable modulo p^{k_0+1}. We remark that not all series f_i are divisible by p, but this is true for every $i \geq s+1$, by definition of s. However, the indices $\text{ind}(n,k,s,\mathbf{i})$ that appear in the statement of Proposition 4.5 are always greater than or equal to $s+1$. Moreover, the sum for h_n in the same Proposition is a finite sum modulo p^{k_0+1}, since it is trivial that $\text{ind}(n,k,s,\mathbf{i}) \geq n+s+k$ and $f_k \equiv 0 \pmod{p^{k_0+1}}$ for every sufficiently large k, as $f_k \to 0$ in $\mathbb{Z}_p\langle x_2\rangle$.
- Finally, we compute $g_0, \ldots, g_s$ modulo p^{k_0+1} using the recursive formulas given above. This can be done since the previous step gave us $h_i \pmod{p^{k_0+1}}$ and, except h_0, every h_i is divisible by p (because $h \in \mathbb{Z}_p\langle x_1, x_2\rangle^\times$), so that the products $g_j h_i$ are computable modulo p^{k_0+1}.

Now that we know how to compute the functions involved in Theorem 4.4 with desired precision, we would like to apply those ideas to the elliptic Chabauty method. We already saw that the elliptic Chabauty method yields $d-1$ formal series in r variables ($d = [K:\mathbb{Q}]$ and r is the rank over K of the elliptic curve we are considering), of which we want to find the common zeros (see Equation 4.1). In our case, $K = \mathbb{Q}(\beta)$ has degree $d = 3$ and E has rank $r = 2$ over K, so we get two formal series $\theta_U^{(1)}, \theta_U^{(2)} \in \mathbb{Z}_p\left[[n_1, n_2]\right]$, which are actually elements of $\mathbb{Z}_p\langle n_1, n_2\rangle$.

Thus, we can apply Theorem 4.4 to $\theta_U^{(1)}$. The formal series $h^{(1)}$ obtained is a unit in $\mathbb{Z}_p\langle n_1, n_2\rangle$ so it can never vanish, therefore $\theta_U^{(1)}(n_1, n_2) = 0$ is equivalent to

$$g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + \ldots + g_s^{(1)}(n_2)n_1^s = 0$$

so that the study of the vanishing of a formal series can be reduced to the study of the zeros of a degree s polynomial with coefficients in $\mathbb{Z}_p\langle n_2\rangle$. In particular, this means that for a fixed n_2, there are at most s zeros of $\theta_U^{(1)}$. By applying the same argument on $\theta_U^{(2)}$, we get a system of two polynomial equations in $\mathbb{Z}_p\langle n_2\rangle\left[n_1\right]$.

Then, the resultant of those polynomials is a formal series in $\mathbb{Z}_p\langle n_2\rangle$, whose zeros can be used to find the common zeros of $\theta_U^{(1)}$ and $\theta_U^{(2)}$. So, it suffices to use Strassman's theorem to bound the number of zeros of the resultant. Finally, we hope that this bound is sharp, meaning that the number of known zeros is exactly equal to the bound, so that there aren't more zeros other than the known ones. This yields a finite

number of values for n_2, which can be then substituted into either one of the equations $g_0^{(i)}(n_2)+g_1^{(i)}(n_2)n_1+\ldots+g_s^{(i)}(n_2)n_1^s=0$. Solve those polynomial equations in n_1 and compute the common zeros, then continue with the elliptic Chabauty method.

Proof of Theorem 4.3

Now that we have developed all the necessary tools, we can return to the proof of theorem 4.3.

Recall that, in order to conclude the proof, we only need to find the points (x, y) on $E(\mathbb{Q}(\beta))$ with $x \in \mathbb{Q}$ on the elliptic curve

$$E : y^2 = F_1(x) = x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1$$

We start by computing the structure of the Mordell-Weil group of E over $K = \mathbb{Q}(\beta)$. With the help of `Magma` we find that $E(K) = \mathbb{Z}G_1 \oplus \mathbb{Z}G_2$, where $G_0 = (0, 1)$ and $G_1 = (1, 1 - \beta^2)$. In this case $p = 3$ satisfies the six conditions outlined at the start of this section.

The orders of the reductions of G_0 and G_1 modulo 3 on the elliptic curve $\widetilde{E}$ are 11 and 33, respectively. In order to have smaller coefficients we use $G_2 = G_0 - 3G_1$ instead of G_0, since G_1, G_2 are generators of $E(K)$ and $\widetilde{G_2}$ has order 1 on $\widetilde{E}$. Hence,following the same notations as before, we can define

- $m_1 = 33$ and $m_2 = 1$, the orders of $\widetilde{G_1}$ and $\widetilde{G_2}$ modulo 3,
- $Q_1 = 33G_1$ and $Q_2 = G_2$, the smallest multiples of the generators which lie in the kernel od the reduction map modulo 3,
- $\mathcal{U} = \{kG_1 : -16 \leq k \leq 16\}$

in such a way that any point $P \in E(K)$ may be written as

$$P = U + n_1Q_1 + n_2Q_2$$

with $U \in \mathcal{U}$ and $n_1, n_2 \in \mathbb{Z}$. Our aim is to find, for each fixed U, the values of $n_1, n_2 \in \mathbb{Z}$ such that P has x-coordinate in $\mathbb{Q}$. First of all, we notice that we can reduce the number of U we need to try: since P has rational x-coordinate and Q_1, Q_2 are in the kernel of the reduction modulo 3, the x-coordinate of $\widetilde{U}$ must be in $\mathbb{F}_3$, but the only elements of $\mathcal{U}$ for which this is true are $\infty, \pm G_1, \pm 3G_1$ and $\pm 14G_1$. Moreover, since P and $-P$ have the same x-coordinate and n_1, n_2 are in $\mathbb{Z}$, we don't need to do computations for both U and $-U$. So we have reduced our problem to finding all the points on $E(K)$ with x-coordinate in $\mathbb{Q}$ which can be written as $U + n_1q_1 + n_2Q_2$, with $n_1, n_2 \in \mathbb{Z}$ and $U \in \mathcal{U}' = \{\infty, G_1, 3G_1, 14G_1\}$.

For each $U \in \mathcal{U}'$ we find the corresponding formal series $\theta_U(n_1, n_2) \in \mathbb{Z}_3[\beta]\langle n_1, n_2\rangle$. Using the appropriate formulas we can compute (see [31] for details) θ_U modulo 3^5 for

every $U \in \mathcal{U}'$, for example:

$$\begin{aligned}\theta_\infty(n_1,n_2) = &\left[189n_1^4 + (81n_2^3+54n_2)n_1^3 + (162n_2^2+108)n_1^2 + (162n_2^3+225n_2)n_1 + (189n_2^4+54n_2^2)\right]\beta^2 + \\ &\left[54n_1^4 + (162n_2^3+162n_2)n_1^3 + 123n_1^2 + (189n_2^3+144n_2)n_1 + (189n_2^4+126n_2^2)\right]\beta + \\ &27n_1^4 + 81n_2^3n_1^3 + (81n_2^2+207)n_1^2 + (27n_2^3+117n_2)n_1 + (189n_2^4+198n_2^2) \pmod{3^5}\end{aligned}$$

In particular, we only need to compute the series which appear as coefficients of β and β^2, which we called $\theta_\infty^{(1)}$ and $\theta_\infty^{(2)}$, respectively.

$$\begin{cases}\theta_\infty^{(1)} = 54n_1^4 + (162n_2^3+162n_2)n_1^3 + 123n_1^2 + (189n_2^3+144n_2)n_1 + (189n_2^4+126n_2^2) \\ \theta_\infty^{(2)} = 189n_1^4 + (81n_2^3+54n_2)n_1^3 + (162n_2^2+108)n_1^2 + (162n_2^3+225n_2)n_1 + (189n_2^4+54n_2^2)\end{cases} \pmod{3^5}$$

We already know that $(n_1, n_2) = (0, 0)$ is a common zero of $\theta_\infty^{(1)}$ and $\theta_\infty^{(2)}$. The results of the previous paragraph and Strassman's theorem allows us (see [31, subsubsection II.4.5.2] for more details) to prove that this is the only common zero over $\mathbb{Z}_3$ (and therefore over $\mathbb{Z}$), so this proves that the only point in $E(K)$ of the form $\infty + n_1Q_1 + n_2Q_2$ with rational x-coordinate is ∞. Similarly, we can prove (see [31, subsubsection II.4.5.1]) that for $U = G_1$ the only solution of

$$\theta_{G_1}^{(1)}(n_1,n_2) = \theta_{G_1}^{(2)}(n_1,n_2) = 0$$

is again $(n_1, n_2) = (0, 0)$ which corresponds to the point $G_1 = (1, 1 - \beta^2)$.

For $U = 3G_1$ the only solution of

$$\theta_{3G_1}^{(1)}(n_1,n_2) = \theta_{3G_1}^{(2)}(n_1,n_2) = 0$$

is again $(n_1, n_2) = (1, 0)$ which corresponds to the point $3G_1 + Q_1 = G_0(0, 1)$.

Finally, for $U = 14G_1$, there are no solution of

$$\theta_{14G_1}^{(1)}(n_1,n_2) = \theta_{14G_1}^{(2)}(n_1,n_2) = 0$$

This proves that the only points on $E(K)$ with rational x-coordinate are $\infty, (0, \pm 1)$ and $(1, \pm(1 - \beta^2))$ and therefore the only possible values for the x-coordinate of a point on $C(\mathbb{Q})$ are 0 and 1, concluding the proof of Theorem 4.3.

4.2 Non-abelian Chabauty

A further generalization of Chabauty's ideas is given by the non-abelian Chabauty method (also called Chabauty-Kim method). The theory behind it is very complex and it would be enough for another thesis, so we are going to give only a short introduction.

Another way to look at the Chabauty method is to embed the curve $\mathcal{C}$ in its Jacobian J with the Abel–Jacobi embedding associated to a rational point $P_0 \in \mathcal{C}(\mathbb{Q})$ and then study the relationships between $\mathbb{Q}_p$-points of $\mathcal{C}$ and the $\mathbb{Q}$-points of J . So we have the following commutative diagram

$$\begin{array}{ccc} \mathcal{C}(\mathbb{Q}) & \hookrightarrow & \mathcal{C}(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}_p) \end{array}$$

Suppose that the Mordell–Weil rank r of $J(\mathbb{Q})$ is strictly less than the genus g of $\mathcal{C}$ and that p is a prime of good reduction for $\mathcal{C}$, then another proof of Chabauty's theorem starts with proving that the image of $\mathcal{C}(\mathbb{Q}_p)$ in the $\mathbb{Q}_p$-vector space $J(\mathbb{Q}_p)\otimes_{\mathbb{Z}}\mathbb{Q}_p$ is dense, while the image of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)\otimes_{\mathbb{Z}}\mathbb{Q}_p$ is contained in the vanishing of some nonzero form f; thus $\mathcal{C}(\mathbb{Q})$ lies in the vanishing locus of f in $\mathcal{C}(\mathbb{Q}_p)$. By the Zariski-density, $f|_{\mathcal{C}(\mathbb{Q}_p)}$ is nonzero, so that its vanishing locus, and therefore also $\mathcal{C}(\mathbb{Q})$, is finite.

On the other hand, Minhyong Kim's idea (see [48], [49], [51], [26]), which was motivated by Grothendieck's anabelian approach, was to replace the Jacobian of $\mathcal{C}$ with a geometric object similar (but more general) to the fundamental group, allowing a variant of Chabauty's argument to work even when r is large. Before we deal with the non-abelian setting, we study the cohomological version of the previous commutative diagram:

$$\begin{array}{ccccc} \mathcal{C}(\mathbb{Q}) & \hookrightarrow & \mathcal{C}(\mathbb{Q}_p) & & \\ \downarrow & & \downarrow & \searrow & \\ H^1_f(G_{\mathbb{Q}}, V_p) & \longrightarrow & H^1_f(G_p, V_p) & \longrightarrow & \mathrm{Lie}(J) \end{array}$$

where $G_{\mathbb{Q}}$ and G_p are the absolute Galois groups of $\mathbb{Q}$ and $\mathbb{Q}_p$, respectively. V_p is the $\mathbb{Q}_p$-Tate module of J and H^1_f denotes the pro-p-Selmer group.

In the Chabauty-Kim method we replace V_p, which is essentially equivalent to the abelianization of the geometric (étale) fundamental group of $\mathcal{C}$, with the $\mathbb{Q}_p$-pro-unipotent completion $\Pi_{\mathcal{C}}$ of the geometric fundamental group of $\mathcal{C}$. Since we would like to work with schemes of finite type, instead of working with $\Pi_{\mathcal{C}}$, we will work with $\Pi_{\mathcal{C},n}$ which is the quotient of $\Pi_{\mathcal{C}}$ by the $(n+1)$-th level of the lower central series of $\Pi_{\mathcal{C}}$.

Kim [49] showed that, for each $n \geq 1$, the spaces $H^1_f(G_{\mathbb{Q}}, \Pi_{\mathcal{C},n})$ and $H^1_f(G_p, \Pi_{\mathcal{C},n})$ can be seen as algebraic varieties over $\mathbb{Q}_p$, which are called the (global and local) Selmer varieties of $\mathcal{C}$. Furthermore, we replace $\mathrm{Lie}(J)$ with the de Rham fundamental group of $\mathcal{C}$, $\Pi^{\mathrm{dR}}_{\mathcal{C}}$ and, as before, we can get some "finite level" version of this fundamental group, denoted by $\Pi^{\mathrm{dR}}_{\mathcal{C},n}$, which, again, can be seen as an algebraic variety over $\mathbb{Q}_p$.

Similarly to the abelian case, there are analogues of the Abel–Jacobi map, which are called by Kim the (local and global) unipotent Albanese maps, Alb_l and Alb_g, respectively. Putting all of this together, we get a commutative diagram

$$\begin{array}{ccccc} \mathcal{C}(\mathbb{Q}) & \hookrightarrow & \mathcal{C}(\mathbb{Q}_p) & & \\ \downarrow{\scriptstyle Alb_g} & & \downarrow{\scriptstyle Alb_l} & \searrow & \\ H^1_f(G_{\mathbb{Q}}, \Pi_{\mathcal{C},n}) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, \Pi_{\mathcal{C},n}) & \xrightarrow{D} & \Pi^{\mathrm{dR}}_{\mathcal{C},n}/\mathrm{F}^0 \end{array}$$

Kim showed that the image of $\mathcal{C}(\mathbb{Q}_p)$ under the map Alb_l is Zariski-dense in the de Rham local Selmer variety $H^1_f(G_p, \Pi_{\mathcal{C},n})$. Suppose the image of the localization map $\log_p := D \circ \mathrm{loc}_p$ is non-Zariski-dense. In other words, there exists an algebraic function F on $\Pi^{\mathrm{dR}}_{\mathcal{C},n}$ which vanishes on the image of $\log_p$. Since the image of $\mathcal{C}(\mathbb{F}_p)$ is Zariski dense, the pullback f of F to $\mathcal{C}(\mathbb{Q}_p)$ is nonzero. But the image of $\mathcal{C}(\mathbb{Q})$ in $\mathcal{C}(\mathbb{Q}_p)$ lies in the vanishing of f, which is necessarily finite. Therefore, $\mathcal{C}(\mathbb{Q})$ is finite as well.

Since $\log_p$ is algebraic, in order to prove the desired non-Zariski density of the image of $\log_p$, it is enough to prove the following "dimension hypothesis" (which is the analogue of the condition $r < g$ in the classical Chabauty method) for $n > 0$:

$$\dim(H^1_f(G_{\mathbb{Q}}, \Pi_{\mathcal{C},n})) < \dim(\Pi^{\mathrm{dR}}_{\mathcal{C},n})$$

To make this method computationally viable, instead of Coleman integrals, we can use iterated Coleman integrals which are more natural to define on Selmer varieties. This allows us to define a sequence of sets

$$\mathcal{C}(\mathbb{Q}) \subseteq \ldots \subseteq \mathcal{C}(\mathbb{Q}_p)_n \subseteq \mathcal{C}(\mathbb{Q}_p)_{n-1} \subseteq \ldots \subseteq \mathcal{C}(\mathbb{Q}_p)_2 \subseteq \mathcal{C}(\mathbb{Q}_p)_1 \subseteq \mathcal{C}(\mathbb{Q}_p)$$

where the set $\mathcal{C}(\mathbb{Q}_p)_n$ can be described by equations in terms of n-fold iterated Coleman integrals.

Clearly, in order to prove that $\mathcal{C}(\mathbb{Q})$ is finite, we only need to prove that $\mathcal{C}(\mathbb{Q}_p)_n$ is finite. This is exactly what Kim conjectured:

Conjecture 4.6 ([49]). *For every n sufficiently large, $\mathcal{C}(\mathbb{Q}_p)_n$ is finite.*

There is strong evidence that this is true and one can prove it if some other conjectures (like the Bloch-Kato conjecture or the Fontaine-Mazur conjecture) are supposed true.

Although this conjecture is enough to prove Faltings' theorem, it does not give any way to actually compute the set $\mathcal{C}(\mathbb{Q})$. However, used together with the Mordell-Weil sieve (see appendix A), this is sufficient to compute the set of rational points in most of the cases (some heuristics by Poonen imply that it should always work). Nevertheless, Kim stated another conjecture that improves the previous one and removes the need for the Mordell-Weil sieve.

Conjecture 4.7 ([4]). *For every n sufficiently large, $\mathcal{C}(\mathbb{Q}_p)_n = \mathcal{C}(\mathbb{Q})$.*

Notice that the two n in the conjectures need to to be the same. For example in the setting of classical Chabauty-Coleman, when $r < g$, we have that $\mathcal{C}(\mathbb{Q}_p)_1$ is finite but there are examples in which $\mathcal{C}(\mathbb{Q}_p)_1 \neq \mathcal{C}(\mathbb{Q})$.

Recently, research on Kim's method has focused on trying to prove the dimension hypothesis unconditionally for larger classes of curves, and making the method more explicit in various ways (e.g. by bounding the number or height of points identified by the method, or using the method to construct and implement practical algorithms for finding integral/rational points). As an example of results that we can expect, we have the following theorem

Theorem 4.8 ([26]). *Let $\mathcal{C}/\mathbb{Q}$ be a smooth, projective and geometrically irreducible curve of genus $g \geq 2$ and suppose that its Jacobian J is isogenous over $\overline{\mathbb{Q}}$ to a product $\prod A_i$ of abelian varieties, with A_i having CM by a number field K_i of degree $2\dim(A_i)$. Then the dimension hypothesis holds for $n \gg 0$ and therefore $\mathcal{C}(\mathbb{Q}_p)_n$ is finite for every sufficiently large n.*

4.2.1 Quadratic Chabauty

In the paragraph above we defined a sequence of sets

$$\mathcal{C}(\mathbb{Q}) \subseteq \ldots \subseteq \mathcal{C}(\mathbb{Q}_p)_n \subseteq \mathcal{C}(\mathbb{Q}_p)_{n-1} \subseteq \ldots \subseteq \mathcal{C}(\mathbb{Q}_p)_2 \subseteq \mathcal{C}(\mathbb{Q}_p)_1 \subseteq \mathcal{C}(\mathbb{Q}_p)$$

We already described the set $\mathcal{C}(\mathbb{Q}_p)_1$ as

$$\mathcal{C}(\mathbb{Q}_p)_1 := \left\{ z \in \mathcal{C}(\mathbb{Q}_p) : \int_{P_0}^{z} \omega = 0, \text{ for every } \omega \in A \right\}$$

and we saw in chapter 1 and 3 that if the Mordell-Weil rank of $J(\mathbb{Q})$ is less than the genus of $\mathcal{C}$, then the set $\mathcal{C}(\mathbb{Q}_p)_1$ is finite and effectively computable. However, if this condition on the rank is not satisfied, then $\mathcal{C}(\mathbb{Q}_p)_1$ could be infinite. In that case, we could study the set $\mathcal{C}(\mathbb{Q}_p)_2$, hoping that it is finite. This is one of the goals of the *Quadratic Chabauty method*, the other being constructing explicit functions on $\mathcal{C}(\mathbb{Q}_p)$ that vanish only on $\mathcal{C}(\mathbb{Q}_p)_2$ (or a finite set containing it).

From a computational point of view, the main idea of quadratic Chabauty is to replace the linear relations in the method of Chabauty–Coleman by bilinear relations, using double Coleman integrals

$$\int_P^Q \omega_i \omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j$$

instead of the classical Coleman integrals that we described in the previous chapters. This can be done using p-adic heights, which were developed by a number of authors, including Néron, Mazur–Tate, Iovita–Werner, Besser, Coleman–Gross and Nekovář (for references see [8, Chapter 2]). For example, we have:

Definition 4.9. The *Coleman-Gross (cyclotomic) p-adic height pairing* is a symmetric bi-additive pairing

$$\begin{aligned} h : \mathrm{Div}^0(\mathcal{C}) \times \mathrm{Div}^0(\mathcal{C}) &\to \mathbb{Q}_p \\ (D_1, D_2) &\mapsto h(D_1, D_2) \end{aligned}$$

defined for all $D_1, D_2 \in \mathrm{Div}^0(\mathcal{C})$ with disjoint support, such that

- We have

$$h(D_1, D_2) = \sum_{v \text{ prime}} h_v(D_1, D_2) = h_p(D_1, D_2) + \sum_{q \neq p} h_q(D_1, D_2)$$

  where $h_p(D_1, D_2)$ can be computed via a Coleman integral of a suitable differential of the third kind and $h_q(D_1, D_2)$ are almost all zero and can be computed using intersection theory.

- For every $g \in \mathbb{Q}(\mathcal{C})^\times$, we have $h(D, \mathrm{div}(g)) = 0$. This implies that h defines a symmetric bilinear pairing $J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$.

This construction was used by Balakrishnan, Besser and Müller to study integral points on certain hyperelliptic curves (see [1, Theorem 3.1] and [8, Section 2.3]), but this approach does not generalize to rational points. To do that we need to use Nekovář's construction of p-adic heights, which uses more difficult tools, like p-adic Hodge theory. For more details on that see Nekovář's original article ([58]), [5] or [8, Chapter 3].

Recall the following definition:

Definition 4.10. The *Néron-Severi group* of J is defined as

$$NS(J) := \mathrm{Pic}(J)/\mathrm{Pic}^0(J)$$

Its rank as $\mathbb{Z}$-module is denoted by $\rho(J)$ and it is called the *Picard number* of J.

Then, using Nekovář's p-adic heights, Balakrishnan and Dogra proved the following theorem:

Theorem 4.11 (Balakrishnan-Dogra, [5, Lemma 3.2])**.** *Suppose that*

$$\mathrm{rank}(J(\mathbb{Q})) < g + \rho(J) - 1$$

Then $\mathcal{C}(\mathbb{Q}_p)_2$ is finite. In particular, this is always true if $\mathrm{rank}(J(\mathbb{Q})) = g$ and $\rho(J) > 1$.

As an application of the Quadratic Chabauty method, we briefly talk about the split Cartan modular curve $X_s(13)$, also known as the "cursed curve", whose model is

$$-x^3y + 2x^2y^2 - xy^3 - x^3z + x^2yz + xy^2z - 2xyz^2 + 2y^2z^2 + xz^3 - 3yz^3 = 0$$

This is a curve of genus $g = 3$ for which $\mathrm{rank}(J(\mathbb{Q})) = 3$, so we cannot apply the classical Chabauty-Coleman method. However, in this case $\rho(J) = 3 > 1$, so we can apply Theorem 4.11 and say that this curve has a finite number of rational points. In 2002, Galbraith found that

$$X_s(13)(\mathbb{Q}) \supseteq \{[0,1,0], [0,0,1], [-1,0,1], [1,0,0], [1,1,0], [0,3,2], [1,0,1]\}$$

but he could not show that this was actually an equality. However, in 2019 this was finally proved using Quadratic Chabauty.

Theorem 4.12 (Balakrishnan-Dogra-Müller-Tuitman-Vonk, [7])**.** *We have*

$$\#X_s(13)(\mathbb{Q}) = 7$$

This theorem shows that Galbraith's list was complete and completes the classification of rational points on split Cartan curves by Bilu-Parent-Rebolledo.

Chapter 5

Applications to Diophantine equations

5.1 A question about triangles

In this section we follow the article by Hirakawa and Matsumura [45]. We will start by ask a question from Euclidean geometry, which will lead to a Diophantine problem that we will be able to solve using the techniques from chapter 2 and a bit of help from `Magma`.

Definition 5.1. A *rational triangle* (resp. *integral triangle*) is a triangle in which each side has rational (resp. integral) length.

As an example, we recall that every rational right triangle has sides of length $k(1 + x^2)$, $k(1 - x^2)$ and $2kx$, where $k, x > 0$ are positive rational numbers.

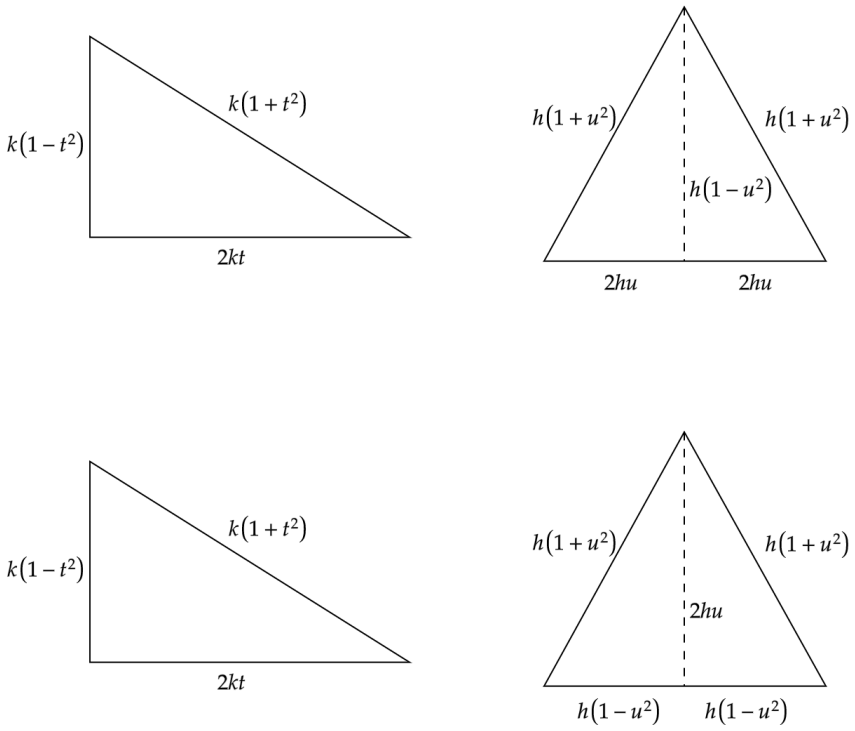
While it is clear that every rational triangle has rational perimeter, there are rational triangles with irrational area (the easiest example being an equilateral triangle with side length 1, which has area $\sqrt{3}/4$). However, perimeter and area are important quantities for a rational triangle, but they don't suffice to uniquely characterize a rational triangle. As a matter of fact, there are a number of works describing infinitely many pairs of rational triangles with the same perimeter and area (see for example [17] and [78]).

We want to prove the following theorem.

Theorem 5.2. *Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with sides of lengths* $(377, 135, 352)$ *and the isosceles triangle with sides of lengths* $(366, 366, 132)$.

Proof. We start by noticing that, since a rational right triangle has always rational area, then the isosceles triangle must have rational area, too. But, if a rational isosceles triangle has rational area, then it must have rational heights and therefore we can divide it

into two copies of a rational right triangle. In other words, using the parametrization of rational right triangles given above, we have have two cases:



where h, k, t, u are positive rational numbers. Since we are considering triangles up to similitude, we can assume that $h = 1$. In the first case, by equating perimeters and area we get the equations

$$\begin{cases} k + kt = 1 + 2u + u^2 \\ k^2 t(1 - t^2) = 2u(1 - u^2) \end{cases}$$

By setting $w = u + 1$ we get the system

$$\begin{cases} t = \dfrac{w^2 - 1}{k} \\ (w^2 - k)w(2k - w^2) = 2k(w - 1)(w - 2); \end{cases}$$

So it is clear that we only need to find the solutions with $w > 1, k > 0$ of the second equation, that is

$$-w^5 + 3kw^3 - 2k^2 w = 2kw^2 - 6kw + 4k$$

or, equivalently

$$2wk^2 + (-3w^3 + 2w^2 - 6w + 4)k + w^5 = 0$$

Since k is a rational number, the discriminant of the equation (as a polynomial in k) must be the square of a rational number, i.e.

$$\Delta = (-3w^3 + 2w^2 - 6w + 4)^2 - 8w^6 = r^2$$

for some rational $r > 0$. This defines an affine curve, whose smooth compactification is an hyperelliptic curve and we will call it by C_1.

It is easy to check that C_1 has at least 10 rational points, namely

$$(w, r) = (0, \pm 4), (1, \pm 1), (2, \pm 8), (12, \pm 868)$$

and the two points at infinity. Notice that we are looking for solution with $w > 1$, so $(w, r) = (0, \pm 4), (1, \pm 1)$ do not give a pair of triangles. Moreover, if $w = 2$ or $w = 12$, then $u = 1$ or $u = 11$, but this implies that the height of the isosceles triangle $1 - u^2$ is not positive. Moreover, we can use the following code in `Magma` to compute the Mordell-Weil rank of the Jacobian J_1 of C_1:

```
> R<w>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve((-3*w^3+2*w^2-6*w+4)^2-8*w^6);
> J:=Jacobian(C);
> RankBounds(J);
```

which gives the outputs `1 1`, i.e. the lower and upper bound for the Mordell-Weil rank of J_1, proving that $\mathrm{rank}(J_1(\mathbb{Q})) = 1$. Now, it's easy to check that C_1 has good reduction at $p = 5 > 2g = 4$ and that $\#C_1(\mathbb{F}_5) = 8$, then theorem 2.17 yields

$$\#C_1(\mathbb{Q}) \leq \#C_1(\mathbb{F}_5) + 2 \cdot 2 - 2 = 10$$

so, this proves that C_1 does not have any other rational points other than the ten listed above, and therefore we don not have any pair of triangles in this case.

In the second case, by the same reasoning as before, we get the system

$$\begin{cases} k + kt = 2 \\ k^2 t(1 - t^2) = 2u(1 - u^2) \end{cases}$$

By multiplying the second equation by k and substituting $t = \frac{2-k}{k}$, we get

$$\begin{cases} k + kt = 2 \\ (2 - k)(2k - 2) = ku(1 - u^2) \end{cases}$$

As above, we only need to solve the second equation, which after expanding looks like this

$$2k^2 + (-u^3 + u - 6)k + 4 = 0$$

and again, by looking at the discriminant, we must have

$$s^2 = (u^3 - u + 6)^2 - 32$$

for some rational number s. This equation defines an affine curve, whose smooth compactification C_2 is an hyperelliptic curve[1]. As before, C_2 has at least 10 rational

[1] Actually, the two curves C_1 and C_2 are isomorphic to each other via the isomorphism induced by the birational map given by $(u, s) = (1 - 2/w, 2r/w^3)$.

points, namely

$$(u,s) = (0,\pm 2), (1,\pm 2), (-1,\pm 2), \left(\frac{5}{6}, \pm\frac{217}{216}\right)$$

and the two points at infinity. In this case, the points $(u,s) = (0,\pm 2), (1,\pm 2), (-1,\pm 2)$ do not give any acceptable pair of triangles, while the other two points give the solutions

$$(k,t,u) = \left(\frac{27}{16}, \frac{5}{27}, \frac{5}{6}\right) \text{ and } \left(\frac{32}{27}, \frac{11}{16}, \frac{5}{6}\right)$$

which correspond to the triangles in the statement, up to similitude. Finally, with the same code as before we can check that $\mathrm{rank}(J_2(\mathbb{Q})) = 1$, and applying again theorem 2.17 with $p = 5$ gives us $\#C_2(\mathbb{Q}) \leq 10$, which means that C_2 has exactly 10 rational points, which are the ones given above. This concludes the proof. □

5.2 A challenge from Serre

Serre, in [64, p. 67], studied Fermat quartics (i.e. Diophantine equations of the form $ax^4 + by^4 = cz^4$, with $a, b, c \in \mathbb{Z}$) and in particular, the special case

$$\mathcal{D}_c : x^4 + y^4 = cz^4$$

where $c \in \mathbb{Z}$ is fourth-power-free. Simple considerations of modular arithmetic imply that if there is a non trivial solution, then any odd prime p dividing c must be congruent to 1 modulo 8 and c must satisfy

$$\begin{aligned} c &\equiv 1, 2 && \pmod{16} \\ c &\not\equiv 3, 4 && \pmod{5} \\ c &\not\equiv 7, 8, 11 && \pmod{13} \\ c &\not\equiv 4, 5, 6, 9, 13, 22, 28 && \pmod{29} \end{aligned}$$

Moreover, it can be shown that these conditions are necessary and sufficient to ensure that the curve $x^4 + y^4 = cz^4$ has points everywhere locally.

So this local considerations allow us to exclude all values of $c \leq 300$ except

$$c \;=\; 1, 2, 17, 82, 97, 146, 226, 257$$

Furthermore, if local considerations fail, then we can use the following maps

$$\begin{aligned} \phi_1 : \quad \mathcal{D}_c &\longrightarrow \mathcal{F}_1 : x^2z^2 + y^4 = cz^4 \\ (x,y,z) &\longmapsto (x^2, yz, z^2) \end{aligned}$$

$$\begin{aligned} \phi_2 : \quad \mathcal{D}_c &\longrightarrow \mathcal{F}_2 : x^4 + y^4 = cx^2z^2 \\ (x,y,z) &\longmapsto (x^2, xy, z^2) \end{aligned}$$

Notice that the curves $\mathcal{F}_1, \mathcal{F}_2$ are both genus 1 curves, therefore their Jacobians are elliptic curves:

$$E_1 : Y^2Z = X^3 + 4cXZ^2 \qquad E_2 : Y^2Z = X^3 - \frac{4}{c^2}XZ^2$$

If we can show that either $E_1(\mathbb{Q})$ or $E_2(\mathbb{Q})$ have rank 0, then it easy to find all points in $\mathcal{D}(\mathbb{Q})$ by inverting the Abel-Jacobi map and ϕ_1 or ϕ_2. This allows to solve the cases $c = 1, 2, 146, 226$, leaving only the cases $c = 17, 82, 97, 257$ (for $c \leq 300$). Notice that in the four remaining cases for c, there are "small" points on $\mathcal{D}_c$, for example: $(2, 1, 1), (3, 1, 1), (3, 2, 1), (4, 1, 1)$, respectively.

Notice that $\mathcal{D}_c$ is always a curve of genus $\frac{(4-1)(4-2)}{2} = 3$ and for $c = 17, 82, 97, 257$ the Jacobian of $\mathcal{D}_c$ has rank 6, so we cannot apply Chabauty's theorem. Serre also tried other approaches, like the Manin-Dem'yanenko method, but for $c = 17, 82, 97, 257$ this is still not applicable.

We will start by proving the following result:

Theorem 5.3 (Flynn, Wetherell [40])**.** *The only rational points on the projective curve*

$$\mathcal{D}_{17} : x^4 + y^4 = 17z^4$$

are $[\pm 1, \pm 2, 1]$ *and* $[\pm 2, \pm 1, 1]$.

First of all, we note that the equation for $\mathcal{D}_{17}$ can be rewritten as

$$\big(17z^2 + (5x^2 - 4xy + 5y^2)\big)\big(17z^2 - (5x^2 - 4xy + 5y^2)\big) = -2(2x^2 - 5xy + 2y^2)^2$$

The two factors on the LHS do not have any common factors on $\mathcal{D}_{17}$, so the double cover of $\mathcal{D}_{17}$ defined by the equations

$$\begin{aligned} 17z^2 + (5x^2 - 4xy + 5y^2) &= dR^2 \\ dR^2\big(17z^2 - (5x^2 - 4xy + 5y^2)\big) &= -2(2x^2 - 5xy + 2y^2)^2 \end{aligned} \tag{5.1}$$

is an unramified cover for every non-zero (squarefree) $d \in \mathbb{Z}$. In other words, any rational point on $\mathcal{D}_{17}$ can be lifted to a rational point on the cover for some value of d. We claim that, up to automorphisms, every rational point corresponds on a rational point on the cover with $d = 34$.

Let $(X, Y, Z) \in \mathcal{D}_{17}(\mathbb{Q})$ so that we can choose X, Y, Z to be coprime integers. Then X and Y cannot be both divisible by 17, since this would imply that $17 \mid Z$; furthermore, if $17 \mid X$, then $Y^4 \equiv 0 \pmod{17}$, which implies $Y \equiv 0 \pmod{17}$. So we can assume that neither X nor Y is divisible by 17.

Moreover, X and Y cannot be both even, because Z would be even too. However, they cannot be both odd, since modulo 4 we would have

$$2 \equiv X^4 + Y^4 = 17Z^4 \equiv Z^4 \equiv 0, 1 \pmod{4}$$

which is impossible. So, without loss of generality, X, Z are odd and Y is even, which implies that $5X^2 - 4XY + 5Y^2$ is positive and congruent to 1 modulo 4. Therefore

$$17Z^2 + (5X^2 - 4XY + 5Y^2) \equiv 2 \pmod{4}$$

which implies that $d \equiv 2 \pmod 4$.

Since $X^4 + Y^4 \equiv (X - 8Y)(X - 2Y)(X + 2Y)(X + 8Y) \equiv 0 \pmod{17}$, we can always assume that

$$2X^2 - 5XY + 2Y^2 = (2X - Y)(X - 2Y) \equiv 0 \pmod{17}$$

after considering $-Y$ instead of Y, if needed. Hence, the product

$$\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big)\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big)$$

must be divisible by 17, which implies that 17 divides at least one of the factors. However, it is easy to see that if one of the factors is divisible by 17, the other is divisible by 17 as well, proving that both factors are divisible by 17.

Lemma 5.4. *At least one between*

$$v_{17}\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) \qquad \textit{and} \qquad v_{17}\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big)$$

is equal to 1. Equivalently, the 17*-adic valuation of the greatest common divisor of* $\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big)$ *and* $\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big)$ *is exactly 1.*

Proof. Recall that

$$v_{17}\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big), v_{17}\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big) \geq 1$$

and that, up to automorphisms, $2X^2 - 5XY + 2Y^2 = (2X - Y)(X - 2Y) \equiv 0 \pmod{17}$. However, $X - 2Y$ and $2X - Y$ cannot be both divisible by 17. Otherwise we would have $X \equiv 2Y \equiv 2(2X) = 4X \pmod{17}$ which implies that $X \equiv 0 \pmod{17}$, contradicting our previous assumptions. So, without loss of generality, we may assume that

$$v_{17}(2X^2 - 5XY + 2Y^2) = v_{17}(2X - Y) = k \geq 1$$

We consider three cases:

- If $k = 1$, then

  $$\begin{aligned} 2 = 2k &= v_{17}(-2(2X^2 - 5XY + 2Y^2)^2) = \\ &= v_{17}\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) + v_{17}\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big) \end{aligned}$$

  Therefore they must be both equal to 1.
- If $k = 2$, then

  $$v_{17}\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) + v_{17}\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big) = 2k = 4$$

  So it suffices to prove that they cannot be both equal to 2.
  Suppose the contrary, so that $17Z^2 + (5X^2 - 4XY + 5Y^2)$ and $17Z^2 - (5X^2 - 4XY + 5Y^2)$ are both divisible by 17^2. Since $v_{17}(2X - Y) = 2$, we have that $Y \equiv 2X \pmod{17^2}$ and thus

  $$\begin{aligned} 17Z^2 + (5X^2 - 4XY + 5Y^2) &\equiv 17Z^2 + 17X^2 \equiv 0 \pmod{17^2} \\ 17Z^2 - (5X^2 - 4XY + 5Y^2) &\equiv 17Z^2 - 17X^2 \equiv 0 \pmod{17^2} \end{aligned}$$

which means that

$$\begin{cases} Z^2 + X^2 \equiv 0 \\ Z^2 - X^2 \equiv 0 \end{cases} \pmod{17}$$

This implies that $X^2 \equiv Z^2 \equiv 0 \pmod{17}$ and therefore $X \equiv Z \equiv 0 \pmod{17}$. Contradiction.

- If $k \geq 3$, then $Y \equiv 2X \pmod{17^k}$ and therefore

$$17Z^4 = X^4 + Y^4 \equiv 17X^4 \pmod{17^k}$$

or, equivalently, $Z^4 \equiv X^4 \pmod{17^{k-1}}$. This implies that $Z^2 \equiv \pm X^2 \pmod{17^{k-1}}$, because $17 \nmid X$. If $Z^2 \equiv X^2 \pmod{17^{k-1}}$, then

$$17Z^2 + (5X^2 - 4XY + 5Y^2) \equiv 34X^2 \pmod{17^{k-1}}$$

Hence, $17 \mid 17Z^2 + (5X^2 - 4XY + 5Y^2)$, but $17^2 \nmid 17Z^2 + (5X^2 - 4XY + 5Y^2)$, because otherwise

$$0 \equiv 17Z^2 + (5X^2 - 4XY + 5Y^2) \equiv 34X^2 \not\equiv 0 \pmod{17^2}$$

as $k-1 \geq 2$ and $17 \nmid X$. Therefore $v_{17}\big(17Z^2+(5X^2-4XY+5Y^2)\big) = 1$. Similarly, if $Z^2 \equiv -X^2 \pmod{17^{k-1}}$, then

$$17Z^2 - (5X^2 - 4XY + 5Y^2) \equiv -34X^2 \pmod{17^{k-1}}$$

and therefore, by the same argument, $v_{17}\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big) = 1$.

□

A consequence of this lemma is that

$$\gcd\left(17Z^2 + (5X^2 - 4XY + 5Y^2), 17Z^2 - (5X^2 - 4XY + 5Y^2)\right)$$

is divisible by 34, and it also divides d. Moreover, d must divide the resultant of the polynomials

$$17z^2 + (5x^2 - 4xy + 5y^2), 17z^2 - (5x^2 - 4xy + 5y^2)$$

which is $28900 = 2^2 \cdot 5^2 \cdot 17^2$.

Lemma 5.5. *d is not divisible by 5.*

Proof. Notice that $17Z^2+(5X^2-4XY+5Y^2), 17Z^2-(5X^2-4XY+5Y^2)$ cannot both be multiples of 5, since otherwise $17Z^2 - 4XY \equiv 17Z^2 + 4XY \equiv 0 \pmod{5}$ which implies that $34Z^2 \equiv 8XY \equiv 0 \pmod{5}$, contradicting our assumption that X, Y, Z are coprime. So we have that at least one between

$$v_5\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) \qquad \text{and} \qquad v_5\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big)$$

is equal to 0.

If $v_5\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) = 0$, then $v_5(dR^2) = 0$.This means that d is not divisible by 5.

If $v_5\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big) = 0$, then we have that

$$v_5\big(-2(2X^2 - 5XY + 2Y^2)^2\big) = 2v_5(2X^2 - 5XY + 2Y^2)$$

is always even. However,

$$\begin{aligned} v_5\big(-2(2X^2 - 5XY + 2Y^2)^2\big) &= v_5\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) + v_5\big(17Z^2 - (5X^2 - 4XY + 5Y^2)\big) \\ &= v_5\big(17Z^2 + (5X^2 - 4XY + 5Y^2)\big) = v_5(dR^2) = v_5(d) + 2v_5(R) \end{aligned}$$

So $v_5(d)$ must be even, but since d is square-free, $v_5(d) = 0, 1$. Therefore $v_5(d) = 0$. □

Combining the previous results, we have that d is square-free, is divisible by 34, but not by 5, and divides $2^2 \cdot 5^2 \cdot 17^2$. This shows that, up to automorphism, every rational point on $\mathcal{D}_{17}$ comes from a rational point on Equation 5.1 with $d = 34$.

So we can rewrite equation 5.1 as

$$\begin{aligned} 17z^2 + (5x^2 - 4xy + 5y^2) &= 34R^2 \\ 17z^2 - (5x^2 - 4xy + 5y^2) &= -68S^2 \\ 2x^2 - 5xy + 2y^2 &= 34RS \end{aligned} \tag{5.2}$$

for some integers R, S. This can be further rearranged as

$$\begin{aligned} (x + y)^2 &= 9(R^2 + 2S^2) - 28RS \\ (x - y)^2 &= R^2 + 2S^2 + 12RS \\ z^2 &= R^2 - 2S^2 \end{aligned} \tag{5.3}$$

The equations 5.3 define a curve of genus 5, which is a cover of the genus 2 curve

$$T^2S^4 = (9R^2 - 28RS + 18S^2)(R^2 + 12RS + 2S^2)(R^2 - 2S^2)$$

In order to prove Theorem 5.3 we only need to show that the only rational points on this curve are the ones with $S = 0$, because

$$(2x - y)(x - 2y) = 2x^2 - 5xy + 2y^2 = 34RS = 0$$

implies that the only points on $\mathcal{D}_{17}(\mathbb{Q})$ are the ones in the statement of the theorem.

By dehomogenizing the equation with respect to S, we get the affine hyperelliptic curve

$$\mathcal{C} : y^2 = (9x^2 - 28x + 18)(x^2 + 12x + 2)(x^2 - 2)$$

of which we hope to find the rational points. In particular, we want to prove that $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-\}$. To do this we could try to apply Chabauty's theorem, but we will see that the Jacobian of $\mathcal{C}$ has Mordell-Weil rank 2.

Instead, we will first prove that the rational points on $\mathcal{C}$ correspond to K-rational points on a suitable genus 1 curve with x-coordinate in $\mathbb{Q}$ and then apply the elliptic Chabauty method.

Proposition 5.6. *Let $\mathcal{C}$ be the genus 2 curve defined over $\mathbb{Q}$ by*

$$\mathcal{C} : y^2 = (9x^2 - 28x + 18)(x^2 + 12x + 2)(x^2 - 2)$$

and let $\mathcal{F}$ be the genus 1 curve defined over $K = \mathbb{Q}(\sqrt{2}, \sqrt{34})$ by

$$\mathcal{F} : v^2 = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2})$$

If $x_0 \in \mathbb{Q}$ is the x-coordinate for some rational affine point $(x_0, y_0) \in \mathcal{C}(\mathbb{Q})$, then it is also the x-coordinate for some K-rational affine point $(x_0, v_0) \in \mathcal{F}(K)$.

This Proposition is the central idea of the proof of theorem 5.3. If we can prove that the set of K-rational points on $\mathcal{F}$ with x-coordinate in $\mathbb{Q}$ is finite and we are able to explicitly compute this set, then we can use this information to compute the set $\mathcal{C}(\mathbb{Q})$. But, before we do that, we need some intermediate results. We define α_1, α_2 to be the roots of $9x^2 - 28x + 18$ and β_1, β_2 to be the roots of $x^2 + 12x + 2$. Then, using 2-descent in `Magma` we can prove the following lemma.

Lemma 5.7. *Let $\mathcal{C}$ the curve of genus 2 defined in Proposition 5.6 and let J be its Jacobian. Then $J(\mathbb{Q}) \cong \mathbb{Z}^2 \times (\mathbb{Z}/2\mathbb{Z})^2$, where the torsion subgroup is generated by the divisors classes*

$$T_1 = [(\alpha_1, 0) - (\alpha_2, 0)] \qquad \textit{and} \qquad T_2 = [(\beta_1, 0) - (\beta_2, 0)]$$

and the quotient group $J(\mathbb{Q})/2J(\mathbb{Q})$ is generated by

$$D_1 = \left[\infty^+ - \infty^-\right] \qquad \textit{and} \qquad D_2 = \left[(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-\right]$$

where x_1, x_2 are the roots of $5x^2 - 18x + 17$ and $y_j = \frac{3(-603x_j + 1187)}{50}$ for $j = 1, 2$.

Proof of Proposition 5.6. Let $F(x) = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2})$ and consider it as a K-rational function on $\mathcal{C}$. The associated divisor of F is $2D$, where

$$D = (\alpha_1, 0) + (\alpha_2, 0) + (-6 + \sqrt{34}, 0) + (\sqrt{2}, 0) - 2\infty^+ - 2\infty^-$$

Let $\mathrm{Div}_D(\mathcal{C}(K))$ be the set of K-rational divisors on $\mathcal{C}$ whose support is disjoint from that of D. We define the homomorphism (notice the similarities with equation 4.2)

$$\begin{aligned} q_F : \mathrm{Div}_D(\mathcal{C}(K)) &\longrightarrow K^\times \\ \sum n_j(x_j, y_j) &\longmapsto \prod F(x_j)^{n_j} \end{aligned}$$

and extend q_F to all K-rational divisors by defining $q_F(\infty^+) = q_F(\infty^-) = 1$ and $q_F((\gamma, 0)) = \left(\frac{F(X)}{X - \gamma}\right)(\gamma)$ if $F(\gamma) = 0$.

Actually, it can be shown that q_F induces a homomorphism (see equation 4.2)

$$\widetilde{q_F} : J(K)/2J(K) \to K^\times/(K^\times)^2$$

This follows from Weil reciprocity and the fact that $\mathrm{div}(F)$ is twice a K-rational divisor (see [61] and [69] for details).

It is easily computed that

$$\widetilde{q_F}(T_1) = \widetilde{q_F}(T_2) = \widetilde{q_F}(D_1) = \widetilde{q_F}(D_2) = 1 \in K^\times/(K^\times)^2$$

which implies that for every $P \in \mathcal{C}(\mathbb{Q})$, $q_F(P) \in (K^\times)^2$.

In particular, if $P = (x_0, y_0) \in \mathcal{C}(\mathbb{Q})$, then $F(x_0) \neq 0$ and $q_F(P) = F(x_0) \in (K^\times)^2$. From this we deduce that there exists $v_0 \in K^\times$ such that

$$v_0^2 = (9x_0^2 - 28x_0 + 18)(x_0 - (-6 + \sqrt{34}))(x_0 - \sqrt{2})$$

which concludes the proof. □

We saw before that an unexpected point on $\mathcal{D}_{17}(\mathbb{Q})$ would give an affine $\mathbb{Q}$-rational point on $\mathcal{C}$ and Proposition 5.6 proved that this implies the existence of a K-rational point on $\mathcal{F}$ with x-coordinate in $\mathbb{Q}$. So, we only need to prove that such points do not exist, which is exactly the content of the next Proposition.

Proposition 5.8. *Let $\mathcal{F}$ as above, then there is no affine point $(x, v) \in \mathcal{F}(K)$ with $x \in \mathbb{Q}$.*

Proof. The curve $\mathcal{F}$ has two K-rational points at infinity, namely ∞^+ and ∞^-. To distinguish them, we will call ∞^+ the point at which v/x^2 is equal to 3. Since $\mathcal{F}$ ha genus 1, we may regard it as an elliptic curve with ∞^+ as the group identity.

Computations in `Magma` show that

$$\mathcal{F}(K) \cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$$

and that the point $P = (-6 + \sqrt{34}, 0)$ is a generator of infinite order.

Let $(x_0, v_0) \in \mathcal{F}(K)$, with $x_0 \in \mathbb{Q}$. In K there are two primes lying over $p = 7$,

$$\mathfrak{p}_1 = (7, 3 - \sqrt{2}) \qquad \text{and} \qquad \mathfrak{p}_2 = (7, 3 + \sqrt{2})$$

both primes are unramified, have the same residue field: $k_1 \cong k_2 \cong \mathbb{F}_{49} = \mathbb{F}_7(\sqrt{34})$ and $\mathcal{F}$ has good reduction at both primes. Let $\mathcal{F}_1, \mathcal{F}_2$ be the reductions of $\mathcal{F}$ at $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively.

It is easy to see that $\mathcal{F}_1(k_1)$ has 36 points, 9 of which have order 3, so that $\mathcal{F}_1(k_1) \cong (\mathbb{Z}/6\mathbb{Z})^2$. Similarly, $\mathcal{F}_2(k_2) \cong \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Moreover, the reduction $P = (-6+\sqrt{34}, 0)$ modulo $\mathfrak{p}_1$ has order 3 in $\mathcal{F}_1(k_1)$, and its reduction modulo $\mathfrak{p}_2$ has order 13 in $\mathcal{F}_2(k_2)$. Since P is a generator of $\mathcal{F}(K)$, we can show that the image of the reduction map $\mathcal{F}(K) \to \mathcal{F}_1(k_1) \times \mathcal{F}_2(k_2)$ has order $4 \cdot 3 \cdot 13$.

Now, let $(x_0, v_0) \in \mathcal{F}(K)$ with $x_0 \in \mathbb{Q}$. Then x_0 reduces to the same value modulo $\mathfrak{p}_1$ and $\mathfrak{p}_2$ (since this is equivalent to reduce modulo $p = 7$), and this value must be in $\mathbb{F}_7 \cup \{\infty\}$. We look for points in $\mathcal{F}(K)$ with the same property, and we do this by computing the reduction of $T + nP$ in $\mathcal{F}_1(k_1) \times \mathcal{F}_2(k_2)$ for every $T \in \mathcal{F}(K)[2]$ and for every $0 \leq n \leq 38$. At the end, we find that the only times $x(T + nP)$ reduces to the same value in $\mathbb{F}_7 \cup \{\infty\}$ at both primes are when that value is ∞. Therefore the denominator of x_0 must be divisible by 7.

Now, we consider only $\mathfrak{p}_1$. With the usual change of variables $s = \frac{1}{x}, t = \frac{y}{x^3}$, the equation for $\mathcal{F}$ becomes

$$\mathcal{F} : t^2 = (18s^2 - 28s + 9)((-6 + \sqrt{34})s - 1)(s\sqrt{2} - 1)$$

Our problem now is to find a point $(s_0, t_0) \in \mathcal{F}(K)$ with $s_0 \in \mathbb{Q}^\times$ and $7 \mid s_0$. By looking at the equation modulo $\mathfrak{p}_1$ we see that $t_0^2 \equiv 9 \pmod{\mathfrak{p}_1}$, so without loss of generality we may assume that $t_0 \equiv 3 \pmod{\mathfrak{p}_1}$.

Since ∞^+ is written as $(0, 3)$ in (s, t)-coordinates, we see that the points we are looking for are exactly the ones which lie in the same residue class of ∞^+. Alternatively, we need to study the set

$$R_{\infty^+} = \{(s, t) \in \mathcal{F}(K_{\mathfrak{p}_1}) : (s, t) \equiv (0, 3) \pmod{\mathfrak{p}_1}\}$$

Assume that $(s, t) \in R_{\infty^+}$. Then we can write $s = 7^i s'$, with $s' \in \mathbb{Z}_{\mathfrak{p}_1}^\times$. Since $\mathfrak{p}_1$ is unramified, we know that the s-coordinate of $7^n m \cdot (s, t)$ is congruent to $7^{i+n} m s'$ modulo 7^{i+n+1}. We will call s' the *leading term* of the point (s, t).

We already know that P has order 3 modulo $\mathfrak{p}_1$, which implies that $3 \cdot P \in R_{\infty^+}$ is non trivial. We can compute $s(3 \cdot P) \equiv 7 \cdot (3 + 2\sqrt{34}) \pmod{7^2}$. Then, since $\mathcal{F}(K)$ has rank 1, we see that any K-rational point in R_{∞^+} is either the identity or its leading term is an integer multiple of $3+2\sqrt{34}$ modulo 7. However, the leading term of (s_0, t_0) is a non zero rational number, hence it cannot involve $\sqrt{34}$ and that's a contradiction.

So we have just proved that there are no points $(s_0, t_0) \in \mathcal{F}(K)$ with the desired properties, and therefore no (x_0, v_0) cannot exists. This implies that there is no affine point $(x, v) \in \mathcal{F}(K)$ with $x \in \mathbb{Q}$, completing the proof of this Proposition and the proof of theorem 5.3.

□

5.3 Generalized Fermat equations

In this section, we want to discuss special instances of generalized Fermat equations, i.e. equation of the form

$$Ax^r + By^s = Cz^t \tag{5.4}$$

where $A, B, C, x, y, z, r, s, t \in \mathbb{Z}$ are all variables, with $A, B, C \neq 0$ and $r, s, t > 0$.

In 1995 Darmon and Granville ([30]) proved that for fixed, nonzero A, B, C and fixed r, s, t satisfying

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$$

the primitive solutions x, y, z correspond to rational points on finitely many algebraic curves, from which follows, by Faltings' theorem, that there are only finitely many primitive solutions. Unfortunately, their proof does not provide a method to produce such curves.

Another important result is due to Tijdeman ([73]), stating that the ABC-conjecture implies that for A, B, C fixed and r, s, t such that $1/r + 1/s + 1/t < 1$, then the number of primitive solutions to $Ax^r + By^s = Cz^t$ is still finite.

However, the case that has received the most attention is the case $A = B = C = 1$. There is an infinite family of exponents (r, s, t) such that the equation 5.4 has primitive solutions, namely $2^3 + 1^s = 3^2$. However, apart from $\{r, s, t\} = \{2, 3, n\}$ there are only 4 other known cases in which there are non zero primitive solutions:

$$\{r, s, t\} = \{2, 3, 7\}, \quad \{2, 3, 8\}, \quad \{2, 3, 9\}, \quad \{2, 4, 5\}$$

In this section we will prove the following theorems (following the article [20]).

Theorem 5.9. *If $x, y, z \in \mathbb{Z}$ satisfy $x^2 + y^4 = z^5$ and $\gcd(x, y, z) = 1$, then $xyz = 0$*

Theorem 5.10. *The only integral, pairwise coprime solutions of $x^2 - y^4 = z^5$ are*

$$(x, y, z) = (0, \pm 1, -1), (\pm 1, 0, 1), (\pm 1, \pm 1, 0), (\pm 7, \pm 3, -2), (\pm 122, \pm 11, 3)$$

Theorem 5.11. *The only integral, pairwise coprime solutions of $x^8 + y^3 = z^2$ are*

$$(x, y, z) = (0, 1, \pm 1), (\pm 1, 0, \pm 1), (\pm 1, -1, 0), (\pm 1, 2, \pm 3), (\pm 43, 96222, \pm 30042907)$$

Before starting we fix some notations. For a number field K, $\mathcal{O}_K$ will denote its ring of integers. For a finite prime $\mathfrak{p}$ of K, we will denote by $K_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of K and by $\mathcal{O}_\mathfrak{p}$ the ring of local integers in $K_\mathfrak{p}$. We will take $v_\mathfrak{p} : K_\mathfrak{p} \to \mathbb{Z}$ as the normalized valuation on $K_\mathfrak{p}$. Moreover, let S be a finite set of primes of K and let L/K be a finite extension. If $\mathfrak{q}$ is a prime of L, then we write $\mathfrak{q} \mid S$ if $\mathfrak{q}$ lies over some prime in S. Otherwise, we write $\mathfrak{q} \nmid S$. We define

$$L(S, m) := \left\{a \in L^\times : v_\mathfrak{q}(a) \equiv 0 \pmod{m}, \text{ for all primes } \mathfrak{q} \nmid S\right\} / (L^\times)^m$$

and

$$\mathcal{O}_{L,S} = \{a \in L : v_\mathfrak{q}(a) \geq 0, \forall \mathfrak{q} \nmid S\}$$

Finally, a tuple $(x_1, \ldots, x_n) \in (\mathcal{O}_L)^n$ is called *S-primitive* if $\min\{v_\mathfrak{q}(x_i) : i = 1, \ldots, n\} = 0$ for all $\mathfrak{q} \nmid S$. If $S = \emptyset$, then an S-primitive tuple is also called *primitive*.

We will call *cover* any non constant map between curves $\varphi : D \to C$. In the following we will allow covers to be ramified. We will say that *D is a cover of C* and we will write D/C if the map φ is obvious. We say that two covers $\varphi_1 : D_1 \to C$ and $\varphi_2 : D_2 \to C$, defined over K, are *isomorphic* if there exists an isomorphism $\psi : D_1 \to D_2$ over K such that $\varphi_1 = \varphi_2 \circ \psi$.

Let $\mathrm{Aut}_K(C)$ be the group of automorphisms of C over K. We will write

$$\mathrm{Aut}(C) = \mathrm{Aut}_{\overline{K}}(C)$$

for an algebraic closure $\overline{K}$ of the field of definition of C. In a similar fashion, we write $\mathrm{Aut}_K(D/C)$ and $\mathrm{Aut}(D/C)$ for the group of automorphisms of the cover D/C. We say that a cover D/C is *Galois* if $\#\mathrm{Aut}(\mathcal{C}) = \deg(D/C)$.

We start by proving a lemma about the parametrization of the solutions of certain Diophantine equations over number fields.

Lemma 5.12. *Let K be a number field, $F, G \in \mathcal{O}_K[X,Y]$ be coprime homogeneous polynomials, $m \in \mathbb{Z}_{\geq 0}$ and $D \in \mathcal{O}_K$. Suppose that S is a set of primes such that*

$$\operatorname{res}(F(X,Y), G(X,Y)), D \in \mathcal{O}_{K,S}^{\times}$$

If $(x,y,z) \in K^3$ is S-primitive and satisfies

$$F(x,y)G(x,y) = Dz^m$$

then there are $z_1, z_2 \in K$, with (z_1, z_2) S-primitive and $\delta_1, \delta_2 \in K(S,m)$ with $\frac{\delta_1\delta_2}{D} \in (K^{\times})^m$ and such that

$$F(x,y) = \delta_1 z_1^m \qquad G(x,y) = \delta_2 z_2^m$$

Proof. Suppose that $\mathfrak{p} \notin S$ is a prime of K, then

$$m v_{\mathfrak{p}}(z) = v_{\mathfrak{p}}\left(\frac{F(x,y)G(x,y)}{D}\right) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$$

since F, G have integral coefficients and $D \in \mathcal{O}_{\mathfrak{p}}^{\times}$. This implies that (x,y) is also S-primitive and therefore, $(x,y) \not\equiv (0,0) \pmod{\mathfrak{p}}$. By hypothesis,

$$v_{\mathfrak{p}}(\operatorname{res}(F(X,Y), G(X,Y))) = 0$$

which means that either $v_{\mathfrak{p}}(F(x,y)) = 0$ or $v_{\mathfrak{p}}(G(x,y)) = 0$. Finally, we have

$$m v_{\mathfrak{p}}(z) = v_{\mathfrak{p}}(Dz^m) = v_{\mathfrak{p}}(F(x,y)G(x,y)) = v_{\mathfrak{p}}(F(x,y)) + v_{\mathfrak{p}}(G(x,y))$$

This means that for every $\mathfrak{p} \nmid S$, $v_{\mathfrak{p}}(F(x,y)), v_{\mathfrak{p}}(G(x,y)) \in m\mathbb{Z}$, proving the existence of z_1, z_2 as in the statement. The existence and the properties of δ_1, δ_2 follow trivially from this. □

Let $F(X,Y) \in \mathcal{O}_K[X,Y]$ be an homogeneous polynomial of degree n and let $D \in \mathcal{O}_K$. We define S to be a (finite) set of primes such that $\operatorname{disc}(F(X,Y)), D \in \mathcal{O}_{K,S}^{\times}$. Up to a change of variables, we can assume that F is monic in X. Let L be a splitting field for $F(X,1)$ over K, so we have $\alpha_1, \ldots, \alpha_n \in L$ such that

$$F(X,Y) = \prod_{i=1}^{n}(X - \alpha_i Y)$$

Suppose that x, y, z is a S-primitive solution in K of the equation $F(X,Y) = DZ^m$. By applying Lemma 5.12 repeatedly over L, we get $\delta_1, \ldots, \delta_n \in L(S,m)$ with $\frac{\delta_1 \cdot \ldots \cdot \delta_n}{D} \in (K^{\times})^m$ and an S-primitive n-uple $(z_1, \ldots, z_n) \in L^n$ such that

$$x - \alpha_i y = \delta_i z_i^m \qquad z = z_1 \cdot \ldots \cdot z_n \sqrt[m]{\frac{\delta_1 \cdot \ldots \cdot \delta_n}{D}}$$

If we eliminate x and y from these equation, we see that $(z_1, \ldots, z_n)$ is a zero of every polynomial in the ideal generated by the set

$$I_\delta := \left\{(\alpha_i - \alpha_j)(\delta_k Z_k^m - \delta_l Z_l^m) - (\alpha_k - \alpha_l)(\delta_i Z_i^m - \delta_j Z_j^m) : 1 \leq i, j, k, l \leq n\right\}$$

Furthermore, the image of $(z_1, \dots, z_n)$ under the map

$$\Phi_\delta : (Z_1, \dots, Z_n) \mapsto \frac{\alpha_j \delta_i Z_i^m - \alpha_i \delta_j Z_j^m}{\delta_i Z_i^m - \delta_j Z_j^m}$$

is K-rational, because it is equal to x/y (notice that by definition of I_δ, the image of Φ_δ does not depend on the choice of i and j).

Bruin, in [20], proved that the model $\mathcal{C}_\delta$ described by I_δ is a smooth projective model of a curve over L in $\mathbb{P}^{n-1}$. This construction is at the heart of the proof of the following theorem.

Theorem 5.13. *Let K, $F(x, y) = Dz^m$ and S as above. Then there is a finite number of Galois-covers $\Phi_P : \mathcal{C}_P \to \mathbb{P}^1$ over K with $\mathrm{Gal}(\mathcal{C}_P/\mathbb{P}^1) \cong (\mathbb{Z}/m\mathbb{Z})^{n-1}$, where $\mathcal{C}_P$ has genus*

$$1 + m^{n-2}\left(\frac{n(m-1)}{2} - m\right)$$

and has good reduction outside $S \cup \{\mathfrak{p} : \mathfrak{p} \mid m\}$, such that

$$\bigcup_{\mathcal{C}_P} \Phi_P(\mathcal{C}_P(K)) = \left\{[x, y] \in \mathbb{P}^1(K) : \exists z \in K \text{ s.t. } F(x, y) = Dz^m \text{ and } (x, y, z) \text{ is } S\text{-primitive}\right\}$$

Moreover, the $\mathcal{C}_P$ are all birational equivalent over $\overline{K}$ and the Φ_P are ramified exactly above the points $[x, y]$ for which $F(x, y) = 0$.

Proof. See [20, pages 31-32]. □

In order to prove Theorem 5.9 and 5.10, we first find a parametrization of the primitive integer solutions of the equations $x^2 \pm u^2 = z^5$, then we write $y^2 = u = U(s, t)$ so that we can apply Theorem 5.13.

Lemma 5.14. *Let $x, u, z \in \mathbb{Z}$ be coprime integers satisfying $x^2 + u^2 = z^5$. Then there are coprime $s, t \in \mathbb{Z}$, such that*

$$\begin{cases} x = t(t^4 - 10t^2s^2 + 5s^4) \\ u = s(s^4 - 10t^2s^2 + 5t^4) \\ z = s^2 + t^2 \end{cases}$$

Proof. Working in $\mathbb{Q}(i)$, we have $x^2 + u^2 = (x + iu)(x - iu)$. Since x, u are coprime, we have $\gcd(x + iu, x - iu) \mid 2$, and therefore $x + iu = \delta(t + is)^5$, for some $\delta \in \mathbb{Z}[i]$ fifth power free which divides 2 and such that its norm is a fifth power. Since $2 = -i(1+i)^2$, δ must be a unit; but every unit in $\mathbb{Z}[i]$ is a fifth power, so we can assume $\delta = 1$. The formulas above follow easily from expanding $(t + is)^5$. □

Lemma 5.15. *Let $x, u, z \in \mathbb{Z}$ be coprime integers satisfying $x^2 - u^2 = z^5$. Then there are $s, t \in \mathbb{Z}$ coprime, such that*

$$\begin{cases} x = \pm\dfrac{s^5 + t^5}{2} \\ u = \dfrac{s^5 - t^5}{2} \\ z = \pm st \end{cases} \qquad \text{or} \qquad \begin{cases} x = \pm(s^5 + 8t^5) \\ u = s^5 - 8t^5 \\ z = \pm 2st \end{cases}$$

Proof. By the usual properties of the gcd, we have:

$$d = \gcd(x+u, x-u) = \gcd(x+u, 2x)$$

Suppose that $d' = \gcd(x, d) \neq 1$, then $d' \mid x$ and $d' \mid d = \gcd(x+u, 2x)$ and therefore $d' \mid x+u$, which implies $d' \mid u$, contradicting $\gcd(x,u) = 1$. So $d' = 1$ and therefore $d = \gcd(x+u, 2x) = \gcd(x+u, 2) = 1, 2$.

If $d = 1$, then $x+u$ and $x-u$ are coprime and therefore $x+u = s^5, x-u = t^5$ for some $s, t \in \mathbb{Z}$, leading to the first parametrization.

If $d = 2$, then there are $\alpha, \beta \in \mathbb{Z}$ coprime such that $x - u = 2\alpha$ and $x + u = 2\beta$, meaning that $4\alpha\beta = z^5$ and therefore, $z = 2\gamma$ for some $\gamma \in \mathbb{Z}$. So $\alpha\beta = 8\gamma^5$ but, since α and β are coprime, we must have

$$\begin{cases} \alpha = s^5 \\ \beta = 8t^5 \end{cases} \qquad \text{or} \qquad \begin{cases} \alpha = 8s^5 \\ \beta = t^5 \end{cases}$$

which lead to equivalent parametrizations, up to exchanging s and t (we have chosen the former to find the formula above). □

So, the previous lemmas imply that any primitive solution to $x^2 \pm y^4 = z^5$ can be obtained from the primitive solutions of one of the equations

$$y^2 = s(s^4 - 10t^2s^2 + 5t^4) \qquad y^2 = \frac{s^5 - t^5}{2} \qquad y^2 = s^5 - 8t^5$$

Using Theorem 5.13, the solutions for the equations above are parametrized by rational points on genus 5 curves. However, those curves cover elliptic curves, so it suffices to find points on those elliptic curves over suitable number fields (see [20, Section 3.3] for details).

In the next three lemmas we will refer to the following table:

j	$\mathcal{E}_j$	$\phi_j(X,Y)$	L
1	$Y^2 = X^4 - 10X^2 + 5$	X	$\mathbb{Q}$
2	$5Y^2 = X^4 - 10X^2 + 5$	X	$\mathbb{Q}$
3	$(-2\beta^3 + 8\beta - 6)Y^2 = \beta^3X^3 + (4\beta^2 - 5)X^2 + (\beta^3 - 4\beta)X - 1$	$1/X$	$\mathbb{Q}(\beta)$
4	$(2\beta^3 - 8\beta - 6)Y^2 = \beta^3X^3 + (4\beta^2 - 5)X^2 + (\beta^3 - 4\beta)X - 1$	$1/X$	$\mathbb{Q}(\beta)$
5	$5Y^2 = X^4 + X^3 + X^2 + X + 1$	X	$\mathbb{Q}$
6	$2(-\zeta^2 + \zeta - 1)Y^2 = X^4 - \zeta X^3 + \zeta^2X^2 - \zeta^3X + \zeta^4$	X	$\mathbb{Q}(\zeta)$
7	$2(\zeta^2 - \zeta + 1)Y^2 = X^4 - \zeta X^3 + \zeta^2X^2 - \zeta^3X + \zeta^4$	X	$\mathbb{Q}(\zeta)$
8	$Y^2 = X^4 + \alpha^3X^3 + 2\alpha X^2 + 2\alpha^4X + 4\alpha^2$	X	$\mathbb{Q}(\alpha)$
9	$(\alpha^3 + \alpha^2 - 1)Y^2 = X^4 + \alpha^3X^3 + 2\alpha X^2 + 2\alpha^4X + 4\alpha^2$	X	$\mathbb{Q}(\alpha)$

where

$$\beta^4 - 5\beta^2 + 5 = 0 \qquad \zeta^4 - \zeta^3 + \zeta^2 - \zeta + 1 = 0 \qquad \alpha^5 - 2 = 0$$

We will only prove Lemma 5.17, as the proofs of the other lemmas are similar.

Lemma 5.16. *The $\{2,5\}$-primitive solutions to $y^2 = s(s^4 - 10t^2s^2 + 5t^4)$ have $s/t = \phi_j(P)$, where $P \in \mathcal{E}_j(L)$ and $j = 1,2,3,4$.*

Lemma 5.17. *The $\{2,5\}$-primitive solutions to $2y^2 = s^5 - t^5$ have $s/t = \phi_j(P)$, where $P \in \mathcal{E}_j(L)$ and $j = 5,6,7$.*

Proof. Let ζ as above, then

$$s^5 - t^5 = (s-t)(s+\zeta t)(s-\zeta^2 t)(s+\zeta^3 t)(s-\zeta^4 t)$$

By applying Lemma 5.12 over $L = \mathbb{Q}(\zeta)$, we see that if there is a $\{2,5\}$-primitive solutions, then there exists $\delta \in L(S,2)$ and rational numbers a_0, a_1, a_2, a_3, a_4 such that:

$$s - t = 2N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\delta)a_4^2$$

$$s + \zeta t = \delta(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3)^2$$

It follows that

$$\left(\frac{s}{t}\right)^4 + \left(\frac{s}{t}\right)^3 + \left(\frac{s}{t}\right)^2 + \left(\frac{s}{t}\right) + 1 = \frac{1}{N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\delta)}\left(\frac{y}{a_4 t^2}\right)^2$$

So, we let $X = s/t$ and we get the equation

$$E_D : DY^2 = X^4 + X^3 + X^2 + X + 1$$

of which we want to find the $\mathbb{Q}$-rational points. However, it's not too difficult to prove that $E_D(\mathbb{Q}) \neq \emptyset$ if and only if $D = 1$ or 5. For $D = 5$ we get the curve $\mathcal{E}_5$.

For $D = 1$, we find an elliptic curve of rank 1, so we need to study the case where the norm $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\delta)$ is a square in more detail. We can take δ a multiplicative combination of $\{2, \zeta^3 + \zeta - 1, \zeta\}$. Local arguments at 2 and 5 show that, without loss of generality, we can take $\delta = \pm(\zeta^3 - 1)$. It follows that for some $y_1 \in \mathbb{Q}(\zeta)$ and $x = s/t$ we have

$$\frac{x^5 - 1}{x + \zeta} = \frac{2N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\delta)}{\delta}y_1^2$$

leading to $\mathcal{E}_6$ and $\mathcal{E}_7$. □

Lemma 5.18. *The $\{2,5\}$-primitive solutions to $y^2 = s^5 - 8t^5$ have $s/t = \phi_j(P)$, where $P \in \mathcal{E}_j(L)$ and $j = 8,9$.*

For Theorem 5.11, we could use the same arguments as above: We first find a parametrization of the solutions of the equation $u^2 - z^2 = -y^3$, where $x^4 = u = U(s,t)$ for some homogeneous polynomial U of degree 3 and then we find parametrizing curves for $x^4 = U(s,t)$. However, Beukers, Edwards and Zagier in [13] and [34] computed parametrizations of $u^4 + y^3 = z^2$, allowing us to state the following lemma.

Lemma 5.19. *Let $x, y, z \in \mathbb{Z}$ be a primitive solution of $x^8 + y^3 = z^2$. Then, there is a C_i from the list below, with $P \in C_i(\mathbb{Q})$ and $t \in \mathbb{Q}$ such that $x = t^3 Y(P)$.*

$$
\begin{aligned}
C_1 &: Y^2 = (X^2 - 3)(X^4 + 18X^2 + 9) \\
C_2 &: Y^2 = -(X^2 - 3)(X^4 + 18X^2 + 9) \\
C_3 &: Y^2 = 6X(X^4 + 12) \\
C_4 &: Y^2 = 6X(3X^4 + 4) \\
C_5 &: Y^2 = X^6 + 40X^3 - 32 \\
C_6 &: Y^2 = -X^6 - 40X^3 + 32 \\
C_7 &: Y^2 = X^6 + 6X^5 - 15X^4 + 20X^3 + 15X^2 + 30X - 17 \\
C_8 &: Y^2 = -X^6 - 6X^5 + 15X^4 - 20X^3 - 15X^2 - 30X + 17 \\
C_9 &: Y^2 = X^6 - 6X^5 + 45X^4 - 180X^3 + 135X^2 + 162X - 405 \\
C_{10} &: Y^2 = -X^6 + 6X^5 - 45X^4 + 180X^3 - 135X^2 - 162X + 405 \\
C_{11} &: Y^2 = 2(X^2 - 3)(X^4 + 18X^2 + 9) \\
C_{12} &: Y^2 = -2(X^2 - 3)(X^4 + 18X^2 + 9)
\end{aligned}
$$

For some of the curves in the lemma above, it is easy to compute their rational points.

Lemma 5.20. $C_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$

Proof. The curve $C_1 : Y^2 = (X^2 - 3)(X^4 + 18X^2 + 9)$ is a double cover of the elliptic curve $Y^2 = (X - 3)(X^2 + 18X + 9)$ by $X \mapsto X^2$. This elliptic curve has only two rational points ∞ and $(3, 0)$, which correspond to the points $\infty^\pm$ and $(\pm\sqrt{3}, 0)$ on C_1, but only the first two are in $C_1(\mathbb{Q})$. □

Lemma 5.21. *The curves $C_2, C_6, C_8, C_{10}, C_{11}$ and C_{12} have no $\mathbb{Q}$-rational points.*

Proof. Each of the curves has no points over $\mathbb{Q}_2$ or $\mathbb{Q}_3$. □

Lemma 5.22. $C_3(\mathbb{Q}) = \{\infty, (0, 0)\}$ *and* $C_4(\mathbb{Q}) = \{\infty, (0, 0)\}$.

Proof. In both cases the curves have the form $Y^2 = Q(X)R(X)$, where $R(X) \in \mathbb{Z}[X]$ has degree 4, so we can use the same argument for both. In particular, we show only the proof for C_3, since the other is the same.

If $X \neq 0, \infty$, then we must have $X^4 + 12 = \delta Y_1^2$ for some $\delta \mid 6$ and $Y_1 \in \mathbb{Q}$. Clearly, $\delta \geq 0$. Let $v_2 : \mathbb{Q} \to \mathbb{Z}$ the usual 2-adic valuation and suppose that δ is even (i.e. $\delta = 2, 6$), then

$$1 + 2v_2(Y) = v_2(\delta Y^2) = v_2(X^4 + 12) \geq \min(4v_2(X), 2)$$

however, since $v_2(X) \in \mathbb{Z}$, we can never have $4v_2(X) = 2$, so the inequality is actually an equality and therefore $v_2(X^4 + 12)$ is always even, contradicting the fact that $v_2(\delta Y^2) = 1 + 2v_2(Y)$ is always odd. So δ must be odd.

Thus we are left with the two elliptic curves

$$X^4 + 12 = Y_1^2 \qquad \text{and} \qquad X^4 + 12 = 3Y_1^2$$

which have both rank 0 with only two rational points: the two points at infinity and $(X, Y_1) = (0, \pm 2)$, respectively. □

We can use a similar argument for the curves C_5, C_7 and C_9. However, the RHS of those equations are irreducible over $\mathbb{Q}$, so we need to work over a suitable extension

Lemma 5.23. *The $\mathbb{Q}$-rational points on C_5, C_7 and C_9 correspond to L-rational points G on the genus 1 covers $\phi = X : \mathcal{E}_j \to \mathbb{P}^1$ with $\phi(G) \in \mathbb{P}^1(\mathbb{Q})$. As $\mathcal{E}_j$ and L we can choose:*

C_j	L	$\mathcal{E}_j$
C_5	$\mathbb{Q}(\rho)$	$\mathcal{E}_{10} : Y^2 = X^4 - 2\rho X^3 + 6\rho^2 X^2 + 8X + 8\rho$
C_7	$\mathbb{Q}(\gamma)$	$\mathcal{E}_{11} : Y^2 = R_1(X)$
C_9	$\mathbb{Q}(\gamma)$	$\mathcal{E}_{12} : Y^2 = R_2(X)$

where $\rho^3 - 2 = 0$, $\gamma^{12} + 6\gamma^{10} + 39\gamma^8 + 64\gamma^6 + 15\gamma^4 - 6\gamma^2 - 3 = 0$, and $R_1, R_2 \in \mathbb{Q}(\gamma)[X]$ have degree 4 (their coefficients are difficult to write, so for their explicit forms we refer to [19, Lemma 4.7.2]).

Proof. Let $F_i(X)$ be the RHS of the equation for the hyperelliptic model of the curve C_i and let L be an extension of $\mathbb{Q}$ such that $F_i = R \cdot Q$ with $R, Q \in L[X]$. Then, if $(x, y) \in C_i(\mathbb{Q})$, there are $\delta, y_1, y_2 \in L$ such that $R(x) = \delta y_1^2$ and $Q(x) = \delta y_2^2$. Without loss of generality, we can take δ square-free S-unit, where S contains the primes dividing $2\mathrm{disc}(F)$ (so there are only finitely many possibilities for δ).

So every rational point on C_i corresponds to an $x \in \mathbb{Q}$ such that $\delta R(x)$ and $\delta Q(x)$ are both squares, however it can be showed that, for all three curves, this happens only if $\delta = 1$.

Finally, since R and Q cannot have degree 1, one of them must have degree 3 or 4 and this is how we find the elliptic curves in the statement. □

Now, thanks to Lemmas 5.17, 5.18, 5.19 and 5.23, we have reduced the problem of proving theorems 5.9, 5.10 and 5.11, to finding the sets $\phi(\mathcal{E}_j) \cap \mathbb{P}^1(\mathbb{Q})$, for $\mathcal{E}_j$ as before. Bruin, in [19, 20], accomplished to compute those intersections by using a slight variation of Elliptic Chabauty (see [20, Section 4] for details). We summarize his results in the following Proposition.

Proposition 5.24. *For each of the curves $\mathcal{E}_j$ above we have*

j	$\phi_j(\mathcal{E}_j(L)) \cap \mathbb{P}^1(\mathbb{Q})$
1	$\{\infty\}$
2	$\{0\}$
3	$\{0\}$
4	$\{0\}$
5	$\{\infty\}$
6	$\{1, -1\}$

j	$\phi_j(\mathcal{E}_j(L)) \cap \mathbb{P}^1(\mathbb{Q})$
7	$\{1, 1/3, 3\}$
8	$\{0, -2, \infty\}$
9	$\{-1\}$
10	$\{0, 1, \infty\}$
11	$\{1/2, \infty\}$
12	$\{9/2, \infty\}$

Now we are ready to prove the main theorems.

Proof of Theorem 5.9. To find the primitive solutions of the equation $x^2 + y^4 = z^5$, we use Lemma 5.14 and 5.16, to reduce the problem to finding the points $P \in \mathcal{E}_j(L)$ with $\phi_j(P) \in \mathbb{P}^1(\mathbb{Q})$, for $j = 1, 2, 3, 4$, and then retrieve the values s and t from that. By using Proposition 5.24, we see that we must have $s/t = \phi_j(P) = 0, \infty$, so either $s = 0$ or $t = 0$, but this implies that $x = 0$ or $y = 0$. □

Proof of Theorem 5.10. To find the primitive solutions of the equation $x^2 - y^4 = z^5$, we use Lemma 5.15, 5.17 and 5.18, to reduce the problem to finding the points $P \in \mathcal{E}_j(L)$ with $\phi_j(P) \in \mathbb{P}^1(\mathbb{Q})$, for $j = 5, 6, 7, 8, 9$, and then retrieve the values s and t from that. By using Proposition 5.24, we get the list of possible values for $s/t = \phi_j(P)$.

By Lemma 5.17, the values of $s/t = \infty, 1, -1$ lead to solutions with $z = 0$, $y = 0$ or $x = 0$, respectively. On the other hand, the values $s/t = 3, 1/3$ lead to the solutions $(x, y, z) = (\pm 122, \pm 11, 3)$.

If $s/t = \infty$ on $\mathcal{E}_8$, we have $t = 0$ and therefore $z = 0$ which was already covered. If $s/t = -2$, then the only pairs of coprime integers s, t are $(s, t) = (2, -1)$ and $(-2, 1)$, and in both cases $s^5 - 8t^5$ is not a perfect square. Finally, if $s/t = -1$ on $\mathcal{E}_9$, we get $s = 1, t = -1$ which corresponds to the solutions $(x, y, z) = (\pm 7, \pm 3, -2)$. □

Proof of Theorem 5.11. Lemma 5.19 implies that the primitive solutions of $x^8 + y^3 = z^2$ are parametrized by rational points on the curves C_i. We know the rational points (or the lack of them) on C_i, for $i = 1, 2, 3, 4, 6, 8, 10, 11, 12$. On these curves the points with $X = 0, \infty$ correspond[2] to solutions with $xyz = 0$, which are easy to find.

On C_5 we still have the point with $X = 1$, namely $(1, \pm 3)$. This point corresponds to the solution

$$(x, y, z) = (\pm 3, 2^3 \cdot 3^2 \cdot 5, \pm 3^3 \cdot 11 \cdot 23)$$

which, unfortunately, is not primitive.

On C_7, the points $\infty^{\pm}$ correspond to $(\pm 1, 2, \pm 3)$ and the points $(1/2, \pm 15/8)$ correspond to $(\pm 3 \cdot 5, 2 \cdot 3^2 \cdot 29 \cdot 37, \pm 3^3 \cdot 99431)$, which is not primitive.

On C_9, the points $\infty^{\pm}$ correspond to $(\pm 3, -2 \cdot 3^2, \pm 3^3)$ and the points $(9/2, \pm 387/8)$ correspond to

$$(\pm 43, 2 \cdot 3 \cdot 7 \cdot 29 \cdot 79, \pm 109 \cdot 275623) = (\pm 43, 96222, \pm 30042907)$$

which is the last of the primitive solutions we were looking for. □

[2] We need to use the Beukers-Edwards-Zagier parametrizations cited before (which can be found in [13, 34]).

Appendix A

The Mordell-Weil sieve

Let $\mathcal{C}/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 2$ and let J be its Jacobian[1]. The *Mordell-Weil sieve* is a method that allows to find information on $\mathcal{C}(\mathbb{Q})$ using information about $J(\mathbb{Q})$ and local information over finite fields.

It was first developed by Scharaschkin in his PhD thesis [62] and later it was adapted and applied by many authors (see [21]). The Mordell-Weil sieve is particularly useful for proving that $\mathcal{C}(\mathbb{Q})$ is empty, but it can be modified to have other applications as well (see for example [21, Section 4]).

Assume that the generators of $J(\mathbb{Q})$ are known and suppose that we can define an Abel-Jacobi map $\iota : \mathcal{C} \to J$ over $\mathbb{Q}$ (that is, we need to know a $\mathbb{Q}$-rational divisor of degree 1 on $\mathcal{C}$). Then, for a prime p of good reduction for $\mathcal{C}$, we have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{C}(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_p} & & \downarrow{\scriptstyle \mathrm{red}_p} \\ \overline{\mathcal{C}}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \overline{J}(\mathbb{F}_p) \end{array}$$

where red_p is the reduction by p map. Notice that if $P \in \mathcal{C}(\mathbb{Q})$, then

$$(\iota_p \circ \mathrm{red}_p)(P) = (\mathrm{red}_p \circ \iota)(P) \in \iota_p(\overline{\mathcal{C}}(\mathbb{F}_p)) \cap \mathrm{red}_p(J(\mathbb{Q}))$$

So, if we can prove that $\iota_p(\overline{\mathcal{C}}(\mathbb{F}_p)) \cap \mathrm{red}_p(J(\mathbb{Q})) = \emptyset$, then $\mathcal{C}(\mathbb{Q}) = \emptyset$ as well.

We can improve this idea in two ways: by working with more than one prime of good reduction at the same time and by using $J(\mathbb{Q})/MJ(\mathbb{Q})$ instead of $J(\mathbb{Q})$ (since the former is a finite group, by Theorem 1.51).

Let S be a finite set of primes of good reduction for $\mathcal{C}$ and $M \geq 2$ an integer. We can extend the commutative diagram above as follows:

[1] In [71] this method is generalized to the case of a subvariety of an abelian variety, but the idea is the same.

$$\begin{array}{ccccc} \mathcal{C}(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) & \xrightarrow{\pi_M} & J(\mathbb{Q})/MJ(\mathbb{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_S} & & \downarrow{\scriptstyle \mathrm{red}_S} & & \downarrow{\scriptstyle \alpha_{S,M}} \\ \prod_{p\in S}\overline{\mathcal{C}}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \prod_{p\in S}\overline{J}(\mathbb{F}_p) & \longrightarrow & \prod_{p\in S}\overline{J}(\mathbb{F}_p)/M\overline{J}(\mathbb{F}_p) \end{array}$$

where we call the composition along the bottom row as $\beta_{S,M}$. Suppose that

$$C_M \subseteq J(\mathbb{Q})/MJ(\mathbb{Q})$$

is a set of residue classes for which we want to show that no rational point $P \in \mathcal{C}(\mathbb{Q})$ maps to C_M under $\pi_M \circ \iota$. Then, the same argument as before shows that it suffices to show that

$$\alpha_{S,M}(C_M) \cap \beta_{S,M}\left(\prod_{p\in S}\overline{\mathcal{C}}(\mathbb{F}_p)\right) = \emptyset$$

In other words, we want to find S such that

$$A(S, C_M) = \left\{ c \in C_M : \alpha_{S,M}(c) \in \beta_{S,M}\left(\prod_{p\in S}\overline{\mathcal{C}}(\mathbb{F}_p)\right)\right\}$$

is empty. Some heuristics by Poonen [59] imply that if $\mathcal{C}(\mathbb{Q}) = \emptyset$, then we can always find a suitable S.

Bibliography

[1] J.S. Balakrishnan, A. Besser, J.S. Müller; *Computing Integral Points on Hyperelliptic Curves Using Quadratic Chabauty*, Mathematics of Computation 86, no. 305 (2016), pp. 1403–1434.

[2] J.S. Balakrishnan, A. Best; *MA: 841 p-adic methods for rational points on curves*, Lecture notes for a course at Boston University (2019), `https://alexjbest.github.io/p-adic-methods/p-adic-methods.pdf`

[3] J.S. Balakrishnan, R. W. Bradshaw, K. Kedlaya; *Explicit Coleman integration for hyperelliptic curves*, in "Algorithmic number theory", volume 6197 of Lecture Notes in Computer Science, Springer (2010) , pp. 16–31.

[4] J.S. Balakrishnan, I. Dan-Cohen, M. Kim, S. Wewers; *A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves*, Mathematische Annalen 372 issue 1-2 (2018), pp. 369–428.

[5] J.S. Balakrishnan, N. Dogra; *Quadratic Chabauty and Rational Points I: p-Adic Heights*, Duke Mathematical Journal 167, no. 11 (2018), pp. 1981–2038.

[6] J.S. Balakrishnan, N. Dogra; *Quadratic Chabauty and Rational Points II: Generalised Height Functions on Selmer Varieties*, International Mathematics Research Notices 2021, no. 15 (2020), pp. 11923–12008.

[7] J.S. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*. Annals of Mathematics 189, no. 3 (2019).

[8] J. Balakrishnan, J.S. Müller; *Computational tools for quadratic Chabauty*, Lecture notes for 2020 Arizona Winter School, `http://math.bu.edu/people/jbala/2020BalakrishnanMuellerNotes.pdf`

[9] J. Balakrishnan, J. Tuitman; *Explicit Coleman integration for curves*, `https://arxiv.org/abs/1710.01673`

[10] F. Baldassarri, B. Chiarellotto; *Algebraic versus rigid cohomology with logarithmic coefficients*, in "Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)", volume 15 of Perspectives in Mathematics (1994), pp. 11–50.

[11] P. Berthelot; *Finitude et pureté cohomologique en cohomologie rigide*, Inventiones Mathematicae 128 (1997), pp. 329-377.

[12] A. Besser; *Heidelberg lectures on coleman integration*, In: The arithmetic of fundamental groups (2012), pp. 3–52.

[13] F. Beukers; *The Diophantine equation* $Ax^p+By^q = Cz^r$, Duke Mathematical Journal 91 (1998), pp. 61–88.

[14] E. Bombieri; *The Mordell conjecture revisited*, Annali della Scuola Normale Superiore di Pisa 17 (1990), pp. 615-640.

[15] S. Bosch; *Lectures on Formal and Rigid Geometry*, Springer Lecture Notes in Mathematics (2014).

[16] N. Bourbaki; *Lie groups and Lie algebras. Chapters 1-3*, Elements of Mathematics, Springer-Verlag (1998).

[17] A. Bremner; *On Heron triangles*, Annales Mathematicae et Informaticae 33 (2006), pp. 15-21.

[18] G. Bresciani, J. Demeio, G. Lido, D. Lombardo; *Lecture notes from a Non-abelian Chabauty study group*, `http://people.dm.unipi.it/lombardo/NonAbelianChabauty/NonabelianChabauty.pdf`

[19] N. Bruin; *Chabauty methods and covering techniques applied to generalized Fermat equations*, PhD dissertation, University of Leiden (1999).

[20] N. Bruin; *Chabauty methods using elliptic curves*, Journal für die reine und angewandte Mathematik vol. 2003, no. 562 (2003).

[21] N. Bruin, M. Stoll; *The Mordell–Weil Sieve: Proving Non-Existence of Rational Points on Curves*, LMS Journal of Computation and Mathematics 13 (2010), pp. 272–306.

[22] C. Chabauty; *Sur les points rationnels des courbes algebriques de genre superieur à l'unité*, Comptes Rendues de l'Academie de Sciences Paris 212 (1941), pp. 882-885.

[23] S. Chan; *Topics in the theory of zeta functions of curves*, Oxford MMath thesis (2016), `https://www.ucl.ac.uk/~ucahytc/chan_dissertation.pdf`

[24] B. Chiarellotto; *Weights in rigid cohomology applications to unipotent* F*-isocrystals*, Annales Scientifiques de l'École Normale Supérieure 31 (Série 4, 1998), pp. 683-715.

[25] J. W. S. Cassels, E. V. Flynn; *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press (1996).

[26] J. Coates, M. Kim; *Selmer varieties for curves with CM Jacobians*, Kyoto J. Math. 50.4 (2010), pp. 827–852.

[27] R. Coleman; *Effective Chabauty*, Duke Math Journal 52 no. 3 (1985), pp. 765-770.

[28] R. Coleman; *Torsion points on curves and p-adic abelian integrals*, Annals of Mathematics 121.1 (1985), pp. 111-168.

[29] R. Coleman, E. de Shalit; *p-adic regulators on curves and special values of p-adic L-functions*, Inventiones mathematicae 93, no. 2 (1988), pp. 239-266.

[30] H. Darmon, A. Granville; *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bulletin of the London Mathematical Society 27 no.6 (1995),pp. 513–543.

[31] S. Duquesne; *Calculs Effectifs des Points Entiers et Rationnels sur les Courbes*, PhD dissertation, Université Bordeaux I (2001).

[32] S. Duquesne; *Points Rationnels et Méthode de Chabauty Elliptique*, Journal de Théorie Des Nombres de Bordeaux 15, no. 1 (2003), pp. 99–113.

[33] B. Edixhoven, G. Lido; *Geometric Quadratic Chabauty*, Journal of the Institute of Mathematics of Jussieu (2021), pp. 1–55.

[34] J. Edwards; *A Complete Solution to $X^2 + Y^3 + Z^5 = 0$*, Journal Für Die Reine Und Angewandte Mathematik 571 (2004), pp. 213-236..

[35] N. D. Elkies; *The Klein quartic in number theory*, The eightfold way, Cambridge University Press (1999), pp. 51-101.

[36] R. Elkik; *Solutions d'equations à coefficients dans un anneau hensélien*, Annales Scientifiques de l'École Normale Supérieure 6 (Série 4, 1973), pp. 553-603.

[37] G. Faltings; *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern [Finiteness theorems for abelian varieties over number fields]*, Inventiones Mathematicae 73, no. 3 (1983), pp. 349–366.

[38] E. V. Flynn; *Coverings of Curves of Genus 2*, Algorithmic Number Theory (2000), pp. 65–84.

[39] E. V. Flynn, J. L. Wetherell; *Finding rational points on biellitpic genus 2 curves*, Manuscripta Mathematicae 100 (1999), pp. 519-533.

[40] E. V. Flynn, J. L. Wetherell; *Covering collections and a challenge problem of Serre*, Acta Arithmetica 98 (2001), pp. 197-205.

[41] W. Fulton; *Algebraic Curves: An Introduction to Algebraic Geometry*, (2008).

[42] S. Gajović ; *Curves with sharp Chabauty-Coleman bound*, Proceedings for the Simons Collaboration "Arithmetic Geometry, Number Theory and Computation" (2020).

[43] F. Q. Gouvêa; *p-Adic Numbers: An introduction (3rd edition)*, Springer Universitext (2020).

[44] R. Hartshorne; *Algebraic Geometry*, Springer Graduate Texts in Mathematics (1977).

[45] Y. Hirakawa, H. Matsumura; *A unique pair of triangles*, Journal of Number Theory 194 (2019), pp. 297-302.

[46] M. Hindry, J. H. Silverman; *Diophantine Geometry*, Springer Graduate Texts in Mathematics (2000).

[47] K. Kedlaya; *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society 16(2001), pp. 323–338. And *errata*, *ibid.* 18 (2003), pp. 417-418.

[48] M. Kim; *The motivic fundamental group of the projective line minus three points and the theorem of Siegel*, Inventiones Mathematicae 161.3 (2005), pp. 629–656.

[49] M. Kim; *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. 45.1 (2009), pp. 89–133.

[50] M. Kim; *A remark on fundamental groups and effective Diophantine methods for hyperbolic curves*, Number Theory, Analysis, and Geometry (In memory of Serge Lang), Springer-Verlag (2012).

[51] M. Kim. *Galois Theory and Diophantine Geometry*, Non-abelian Fundamental Groups and Iwasawa Theory, London Mathematical Society Lecture Note Series, Vol. 393, Cambridge University Press (2012), pp. 162–187.

[52] B. Lawrence, A. Venkatesh; *Diophantine Problems and p-Adic Period Mappings*, Inventiones Mathematicae 221, no. 3 (2020), pp. 893–999.

[53] A. Mattuck; *Abelian varieties over p-adic ground fields*, Annals of Mathematics 2 (1955), pp. 92-119.

[54] W. McCallum, B. Poonen; *The method of Chabauty and Coleman*, Explicit methods in number theory (2012), pp. 99–117.

[55] R. Menares; *Lecture notes on Tate algebras*, `http://www.mat.uc.cl/~rmenares/TateAlgebras.pdf`

[56] J. S. Milne; *Jacobian varieties*, Arithmetic geometry (1986), pp. 167 - 212.

[57] L. Mordell; *On the rational solutions of the indeterminate equation of the third and fourth degree* Mathematical Proceedings of the Cambridge Philosophical Society Vol. 21 (1992).

[58] J. Nekovář; *On p-Adic Height Pairings*, Séminaire de Théorie Des Nombres Paris 1990–91 (1993), pp. 127–202.

[59] B. Poonen; *Heuristics for the Brauer–Manin Obstruction for Curves*, Experimental Mathematics 15, no. 4 (2006), pp. 415–420.

[60] B. Poonen, E.F. Schaefer; *Explicit Descent for Jacobians of Cyclic Coevers of the Projective Line* Journal Für Die Reine Und Angewandte Mathematik, no. 488 (1997), pp. 141–188.

[61] E.F. Schaefer; *Computing a Selmer group of a Jacobian using functions on the curve*, Mathematische Annalen 310 issue 3 (1998), pp. 447–471.

[62] V. Scharaschkin; *Local-global problems and the Brauer-Manin obstruction*, PhD dissertation, University of Michigan (1999).

[63] P. Schneider; *Basic notions of rigid analytic geometry*, Galois representations in arithmetic algebraic geometry (1996), volume 254 of London Math. Soc. Lecture Note Ser., pp. 369–378.

[64] J.P. Serre; *Lectures on the Mordell-Weil Theorem*, Aspects of Mathematics (1997).

[65] I. R. Shafarevich; *Basic Algebraic Geometry 1*, Springer (2013).

[66] S. Siksek; *Explicit Chabauty over Number Fields*, Algebra & Number Theory 7, no. 4 (2013), pp. 765–793.

[67] S. Siksek; *Chabauty and the Mordell-Weil Sieve*, Advances on Superelliptic Curves and Their Applications (2015), pp. 194-224.

[68] J. H. Silverman; *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics (2009).

[69] M. Stoll; *Implementing 2-Descent for Jacobians of Hyperelliptic Curves*, Acta Arithmetica 98, no. 3 (2001), pp. 245–277.

[70] M. Stoll; *Independence of rational points on twists of a given curve*, Compositio Mathematica 142 (2006), pp. 1201 - 1214.

[71] M. Stoll; *Applications of the Mordell-Weil sieve*, Oberwolfach Report 34/2007, Oberwolfach Reports 4 (2007), pp. 1967-1970.

[72] T. Sugatani; *Rings of Convergent Power Series and Weierstrass Preparation Theorem*, Nagoya Mathematical Journal 81 (1981), pp. 73–78.

[73] R. Tijdeman; *Diophantine equations and Diophantine approximations*, Number theory and applications (1989), pp. 215–243.

[74] N. Triantafillou; *Restriction of scalars, the Chabauty-Coleman method, and* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, PhD dissertation, MIT (2019).

[75] J. Tuitman; *Counting points on curves using a map to* $\mathbb{P}^1$*, I*, Mathematics of Computation 85, no. 298 (2015), pp. 961–981.

[76] J. Tuitman; *Counting points on curves using a map to* $\mathbb{P}^1$*, II*, Finite Fields and Their Applications 45 (2017), pp.301–322.

[77] M. van der Put; *The cohomology of Monsky and Washnitzer*, Mémoires de la Société Mathématique de France 23 (1986), pp. 33-59.

[78] R. van Luijk; *An elliptic K3 surface associated to Heron triangles*, Journal of Number Theory 123 (2007), no. 1, pp.92-119.

[79] P. Vojta; *Siegel's theorem in the compact case*, Annals of Mathematics 133 (1991), pp. 509-548.

[80] J. L. Wetherell; *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD dissertation, University of California at Berkeley (1997).